



EDGE Router ER 75i,
ER 75i DUO und ER 75i SL
BENUTZERHANDBUCH





ISO 9001:2001



Inhalt

Angewandte Symbole



Gefahr – wichtiger Hinweis, der die Sicherheit der Person oder die Funktionstüchtigkeit des Geräts beeinflussen kann.



Vorsicht – Hinweis auf mögliche Probleme, die in spezifischen Fällen auftreten können.



Information, Anmerkung – Informationen, die nützliche Ratschläge oder interessante Anmerkungen enthalten.

GPL Lizenz

Die Quellencodes, auf die sich die GPL Lizenz bezieht, können gebührenfrei nach der Zusendung des Antrags an die Anschrift info@conel.cz bezogen werden.

Conel s.r.o., Sokolská 71, 562 04 Ústi nad Orlicí, Tschechische Republik
Herausgegeben in der Tschechischen Republik, 11.8.2009



1. Sicherheitshinweise

Bitte beachten Sie folgende Hinweise:

- Der Router muss in Übereinstimmung mit sämtlichen gültigen internationalen sowie nationalen Gesetzen oder mit jeglichen speziellen, den Einsatz in vorgeschriebenen Anwendungen und Umgebungen regelnden Beschränkungen verwendet werden.
- Verwenden Sie nur für den Router bestimmtes Originalzubehör. Somit beugen Sie möglichen Gesundheitsschäden und Gerätebeschädigungen vor und stellen die Einhaltung aller einschlägigen Bestimmungen sicher. Nicht autorisierte Anpassungen oder Anwendung eines nicht zugelassenen Zubehörs können die Beschädigung des Routers sowie die Verletzung der gültigen Vorschriften zur Folge haben. Die Anwendung von nicht zugelassenen Anpassungen oder vom nicht zugelassenen Zubehör kann die Aufhebung der Garantiegültigkeit zur Folge haben.
- Der Router darf nicht geöffnet werden. Es ist nur der Austausch der SIM Karte erlaubt.



- Vorsicht! Kleine Kinder könnten die SIM Karte verschlucken.
- Die Spannung auf dem Versorgungsstecker des Routers darf nicht überschritten werden.
- Setzen Sie den Router nicht extremen Umgebungsbedingungen aus. Schützen Sie das Gerät vor Staub, Feuchtigkeit und Hitze.
- Es wird empfohlen den Router nicht in der Nähe von Tankstellen zu benutzen. Wir weisen die Benutzer darauf hin, die Einschränkungen, die die Anwendung von Funkanlagen in Tankstellen, Chemiewerken oder bei Sprengungen betreffen, zu beachten.
- Bei Flugreisen schalten Sie den Router aus. Die Benutzung des Routers in Flugzeugen kann den Flugzeugbetrieb gefährden, das Mobilnetz stören und gesetzwidrig sein. Die Nichteinhaltung dieser Hinweise kann die Beanstandung oder Aufhebung der telefonischen Dienstleistungen bei diesem Kunden, rechtliche Schritte oder beiden dieser Möglichkeiten zur Folge haben.
- Bei der Anwendung des Routers in der Nähe von persönlichen medizinischen Geräten, wie z. B. Herzschrittmachern oder Hörgeräten, müssen Sie auf erhöhte Vorsicht achten.
- In der Nähe von Fernsehgeräten, Rundfunkgeräten und Personalcomputern kann der Router Störungen hervorrufen.



2. Beschreibung des Routers ER 75i, ER 75i DUO und ER 75i SL

2.1. Einleitung

Der EDGE Router ist ein kompaktes auf Modulbasis gebautes elektronisches Gerät, das Datenübertragungen mittels der Technologien GSM, GPRS und EDGE ermöglicht.

Vor allem erweitert der Router die Möglichkeiten des GSM / GPRS / EDGE Moduls um den Anschluss von mehreren PCs über eine eingebaute Ethernet-Schnittstelle. Darüber hinaus stellt die Router-Firmware den automatischen Aufbau und die Erhaltung der GPRS Verbindung sicher. Durch die Integrierung des DHCP Servers ermöglicht der Router den Benutzern eine einfache Installation und den Zutritt zum Internet.

Der Router ist gleichzeitig mit der USB 2.0 Schnittstelle in Vollgeschwindigkeit ausgestattet, diese Schnittstelle ist für den Anschluss an PCs mit dem Betriebssystem Windows 2000, XP und Vista vorgesehen. Zur Inbetriebnahme dieser Schnittstelle reicht es aus, auf dem PC die Treiber von der mitgelieferten CD zu installieren.

Auf Kundenwunsch ist es möglich, den Router mit dem Portmodul PORT1 auszustatten und somit die Funktionstüchtigkeit des Geräts zu erweitern. Auf diese Weise kann der Router mit der seriellen Schnittstelle RS232, RS485/RS422, M-BUS oder mit dem CNT (E/A Modul) ergänzt werden.

Den Router EDGE gibt es in drei Varianten. Die Grundversion des Routers ist die ER 75i, die Version ER 75i DUO bietet die Möglichkeit, zwei SIM Karten zur Verbindung mit dem GSM Netz zu nutzen, und die Version ER 75i SL ist die Grundversion des Routers mit einem Aluminiumgehäuse. Alle Versionen des Routers nutzen die gleiche Firmware.



Beispiele für mögliche Anwendungen

- mobiles Büro
- Bildübertragung
- Sicherheitssysteme
- Telematik
- Telemetrie
- Fernüberwachung
- Verfolgen von Verkehrsinformationen
- Verkaufs- und Ausgabeautomaten

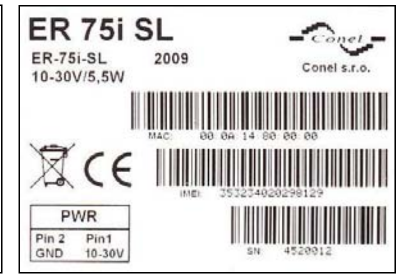
2.2. Markierung der Lieferung

Schildmuster

Handelsbezeichnung	Typenbezeichnung	Sonstiges
ER 75i	ER-75i	Variante mit 1 SIM
ER 75i DUO	ER-75i-DUO	Variante mit 2 SIM
ER 75i SL	ER-75i-SL	Variante mit Aluminiumgehäuse



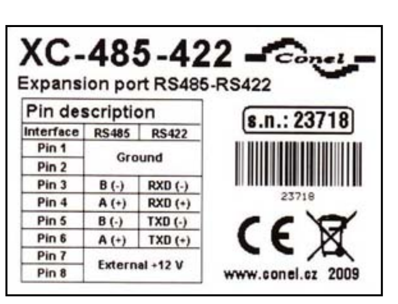


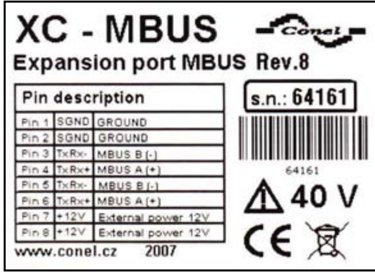


Schildmuster des Erweiterungsanschlusses PORT1:

Handelsbezeichnung des Anschlusses PORT1	Typenbezeichnung	Stromversorgung
Expansion Port RS232	XC-232	Interne Stromversorgung
Expansion Port RS485-RS422	XC-485-422	Interne / externe Stromversorgung
Expansion Port MBUS	XC-MBUS	Externe Stromversorgung
Expansion Port CNT	XC-CNT	Interne Stromversorgung











Der Standardtyp des Routers enthält im Lieferumfang:

- eigenen EDGE Router ER 75i oder ER 75i DUO oder ER 75i SL,
- netzteil,
- UTP Kabel, querverdrahtet,
- externe, magnetische Stabantenne,
- kunststoffelemente zur Befestigung auf der DIN Schiene mit Befestigungsschrauben,
- installations-CD mit Anleitung und Treibern.



Zum Standardtyp kann weiteres Zubehör bestellt werden

- Erweiterungsanschluss RS232, RS485/422, M-BUS oder CNT (die den Abstand haltende Säulen sind im Lieferumfang enthalten),
- Kabel USB A-B.



Router ist vorgesehen:

- zur Montage auf die Montageplatte mithilfe von Durchgangsbohrungen (nur bei Versionen ER 75i und ER 75i DUO),
- beziehungsweise zum Auflegen auf die Arbeitsfläche
- zur Montage auf die DIN Schiene mit Befestigungselementen aus Kunststoff

2.3. Antennenanschluss

Die externe Stabantenne wird an den Router über den FME Stecker auf der Rückplatte angeschlossen.

Beispiel für eine Antenne:



2.4. SIM Kartenleser

Auf der Frontplatte des Routers wird der SIM Kartenleser zum Lesen der SIM Karten 3 V und 1,8 V untergebracht. Zur Inbetriebnahme des Routers ist es notwendig, die aktivierte SIM Karte mit entsperrtem PIN Code in den Kartenleser einzulegen.



1. Vergewissern Sie sich, dass der Router nicht unter Spannung steht.
2. Lassen Sie den Leserhalter durch Betätigung der kleinen gelben Taste neben dem Leser herausfahren.
3. Legen Sie die SIM Karte in den Leserhalter ein und lassen Sie ihn in den Leser hineinfahren.

2.5. Stromversorgung

Der Router braucht eine Gleichstromversorgung +10 bis +30 V. Der Router hat einen eingebauten Schutz gegen Verpolung ohne Anzeige.

Beim Empfang beträgt der Verbrauch 1 W. Bei Datensendung beträgt der Wert des Spitzenverbrauchs 5,5 W. Für die richtige Funktion ist es notwendig, dass das Netzteil für Stromversorgung imstande ist, Spitzenstrom von 500 mA zu liefern.

2.6. Technische Parameter

GSM Modul		MC75i
Entspricht den Normen		EN 301 511, v9.0.2 ETSI EN 301 489-1 V1.8.1 EN 60950-1:06 ed.2
Frequenzbereiche		EGSM850, EGSM900, GSM1800 und GSM1900 aufgrund von VO-R/1/12.2008-1
Sendeleistung		Klasse 4 (2 W) für EGSM850 Klasse 4 (2 W) für EGSM900 Klasse 1 (1 W) für EGSM1800 Klasse 1 (1 W) für EGSM1900
Temperaturbereich	Funktion Lagerung	-20 °C bis +55 °C -40 °C bis +85 °C
Versorgungsspannung		10 bis 30 V Gleichspannung
Verbrauch	Empfang Senden	1 W 5,5 W
Abmessungen	ER 75i, ER 75i DUO ER 75i SL	30 x 90 x 102 mm (Befestigung auf DIN Schiene 35 mm) 42 x 86 x 94 mm (Befestigung auf DIN Schiene 35 mm)
Gewicht		140 g
Antennenstecker		FME – 50 Ohm
Benutzerschnittstelle	ETH USB PORT1	Ethernet – Stecker RJ45 (10/100 Mbit/s) USB 2.0 – Stecker USB-B Optionen – Stecker RJ45 (150 b/s – – 230 400 b/s), RS232, RS485/422, M-BUS, CNT

2.7. Beschreibung der einzelnen Routerteile

2.7.1. GSM/GPRS/EDGE Modul

Für die drahtlose Kommunikation im GSM Netz wird ein Cinterion Modul angewandt. Es wird direkt auf der Platte der gedruckten Schaltungen integriert. Der herausschiebbare Halter des SIM Kartenlesers ist von der Frontplatte aus erreichbar. Der Antennenstecker ist von der Rückplatte aus erreichbar.

Das GSM/GPRS/EDGE Modul ist mit einer USB 2.0 Schnittstelle in Vollgeschwindigkeit ausgestattet, diese Schnittstelle wird auf den mit USB gekennzeichneten Stecker USB-B ausgeführt. An den Steuercomputer wird das Modul über die serielle Hochgeschwindigkeitsschnittstelle RS-232 angeschlossen

GSM/GPRS/EDGE Modul

- Das Modul kommuniziert in vier GSM Bereichen (850 MHz, 900 MHz, 1800 MHz und 1900 MHz).
- Im GPRS Modus ist das Modul imstande, in drei „Time Slots“ zu senden und in zwei zu empfangen (GPRS Multi-Slot Class 10 – Maximalgeschwindigkeit in Bits beim Empfang beträgt 42,8 kb/s) oder in einem „Time Slot“ zu senden und in vier zu empfangen (GPRS Multi-Slot Class 12 – Maximalgeschwindigkeit in Bits beim Empfang beträgt 85,6 kb/s).
- Im EDGE Modus ist das Modul imstande, in drei „Time Slots“ zu senden und in zwei zu empfangen (EDGE Multi-Slot Class 10 – Maximalgeschwindigkeit in Bits beim Empfang beträgt 118,4 kb/s) oder in einem „Time Slot“ zu senden und in vier zu empfangen (EDGE Multi-Slot Class 12 – Maximalgeschwindigkeit in Bits beim Empfang beträgt 236,8 kb/s).
- Es unterstützt das Codierungsschema CS1 bis CS4 und MCS1 bis CS9.



Vorsicht! Das Senden und der Empfang in Time Slots sind von den Möglichkeiten des Netzbetreibers abhängig.

2.7.2. Steuerungsmikrocomputer

Den Kern des Routers bildet ein 32-Bit Mikroprozessor mit 16 MB RAM, 4 MB FLASH EEPROM, serieller Schnittstelle RS-232 und Ethernet Schnittstelle 10/100 Mbit/s. Der Mikrocomputer wird über die serielle Schnittstelle an das OEM Cinterion Modul angeschlossen und steuert die Kommunikation über GSM/GPRS. In Richtung zum Benutzer ist es an eine Ethernet Schnittstelle angeschlossen.

Die Programmausstattung wird über das Betriebssystem uClinux aufgebaut.

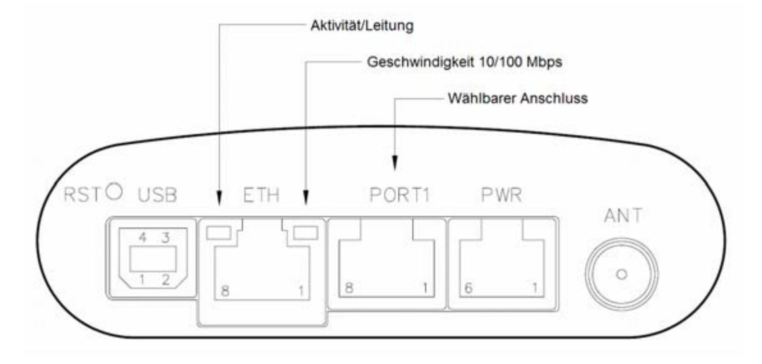
Der Router bietet Dienste wie DHCP, NAT, GRE, IPsec Tunnel, und weitere an.

Die Routereinstellung wird im FLASH EEPROM Speicher hintergelegt. Jegliche Router Konfiguration kann über die Webschnittstelle (HTTP) erfolgen, die mit einem Passwort abgesichert ist.

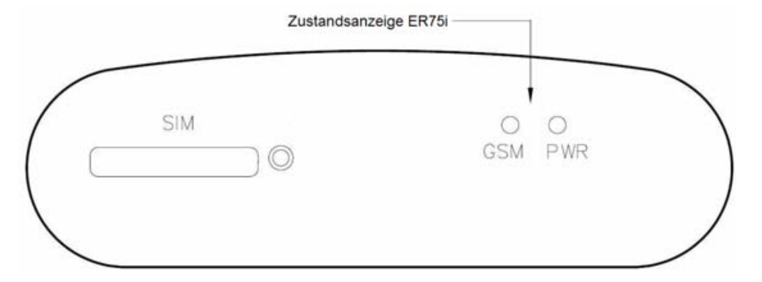
2.8. *Benutzerschnittstellen (Stecker)*

Auf der Rückplatte des Routers befinden sich:

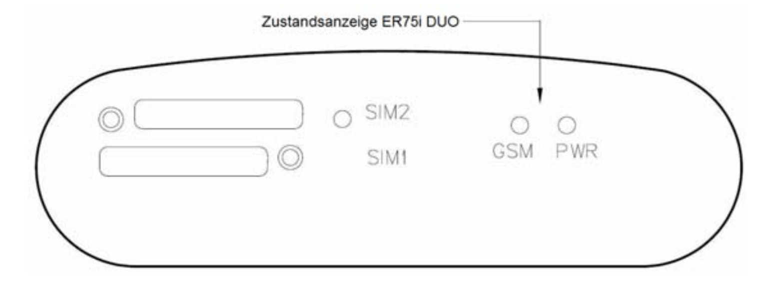
- ein Stecker RJ12 oder MRT9 (PWR) – zum Anschluss des Stromversorgungsadapters,
- ein Stecker RJ45 (ETH) – zum Anschluss an das lokale Computernetz,
- ein Stecker RJ45 (Optionsanschluss PORT1) – zum Anschluss der Geräte über RS232, RS485/422, M-BUS oder CNT
- ein Stecker FME (ANT) – zum Antennenanschluss,
- ein Stecker USB-B (USB) – zum Anschluss des Routers an den PC.



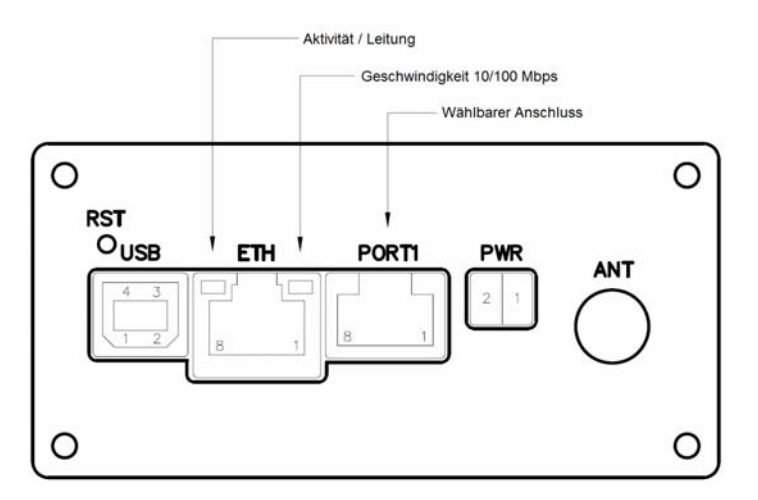
Rückplatte von ER 75i und ER 75i DUO



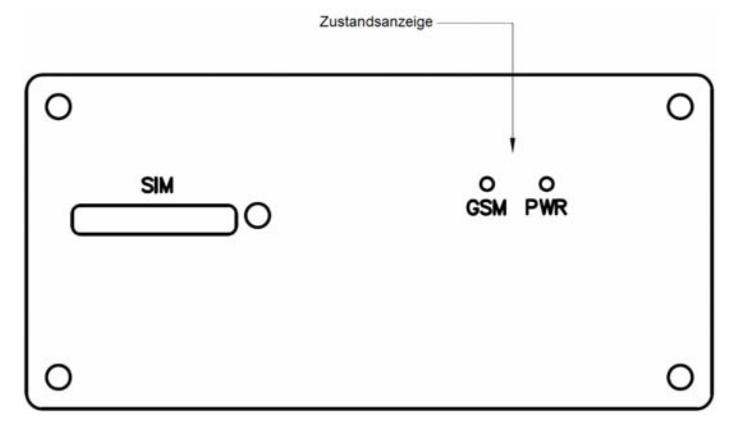
Frontplatte von ER 75i



Frontplatte von ER 75i DUO



Rückplatte von ER 75i SL



Frontplatte von ER 75i SL

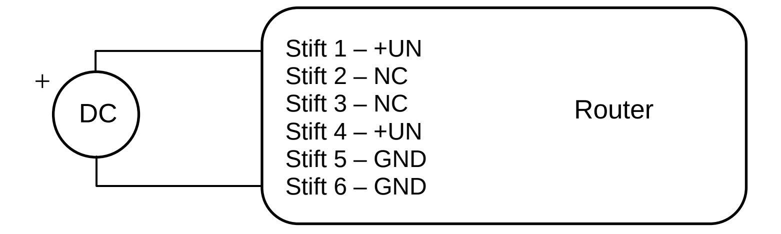
2.8.1. Belegung des PWR Stromversorgungssteckers

- Gerätebuchse RJ12

Stiftnummer	Signalbezeichnung	Beschreibung
1	+UN	Pluspol der Versorgungsgleichspannung (+10 bis +30 V)
2	NC	Signal nicht belegt
3	NC	Signal nicht belegt
4	+UN	Pluspol der Versorgungsgleichspannung (+10 bis +30 V)
5	GND	Minuspol der Versorgungsgleichspannung
6	GND	Minuspol der Versorgungsgleichspannung



Belegungsbeispiel:

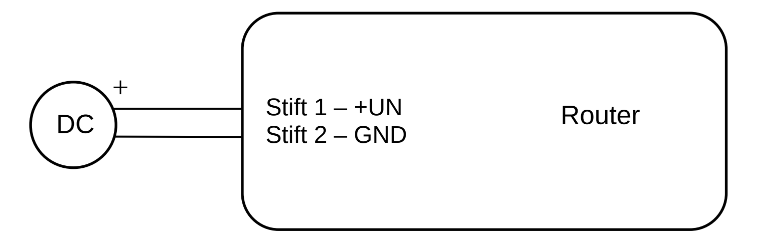


- Gerätebuchse MRT9

Stiftnummer	Signalbezeichnung	Beschreibung
1	+UN	Pluspol der Versorgungsgleichspannung (10 bis 30 V)
2	GND	Minuspol der Versorgungsgleichspannung



Belegungsbeispiel:





Auf dem Versorgungsnetzteil ist +UN mit roter Hülse gekennzeichnet.

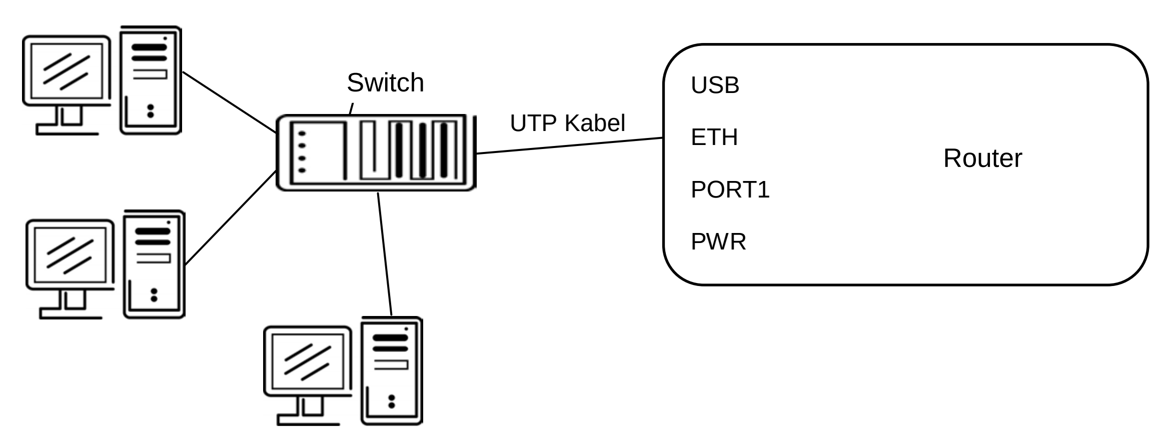
2.8.2. Belegung des Steckers ETH

Gerätebuchse RJ45

Stiftnummer	Signalbezeichnung	Beschreibung	Datenflussrichtung
1	TXD+	Transmit Data – Pluspol	Eingang / Ausgang
2	TXD-	Transmit Data – Minuspol	Eingang / Ausgang
3	RXD+	Receive Data – Pluspol	Eingang / Ausgang
4	---	---	
5	---	---	
6	RXD-	Recieve Data – Minuspol	Eingang / Ausgang
7	---	---	
8	---	---	

Vorsicht! Der ETH Anschluss ist mit POE (Power Over Ethernet) nicht kompatibel!


Belegungsbeispiel beim ETH Router:

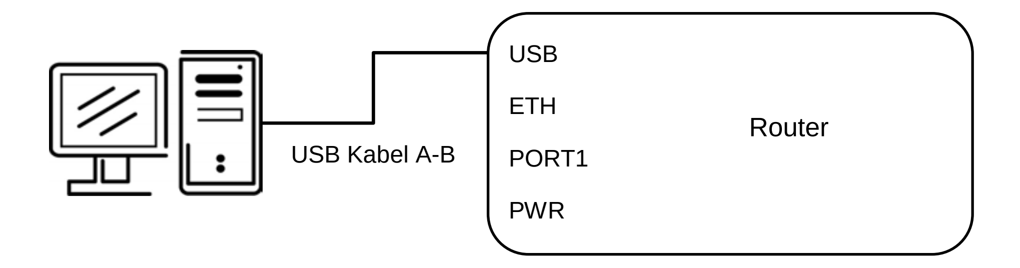


2.8.3. Belegung des Steckers USB

Gerätebuchse USB-B

Stiftnummer	Signalbezeichnung	Beschreibung	Datenflussrichtung
1	VCC	Pluspol der Versorgungsgleichspannung 5 V	
2	USB Data -	Datensignal USB - Minuspol	Eingang / Ausgang
3	USB Data +	Datensignal USB - Pluspol	Eingang / Ausgang
4	GND	Minuspol der Versorgungsgleichspannung	


Belegungsbeispiel beim USB Router:



2.8.4. Steckerbelegung beim Erweiterungsanschluss PORT1

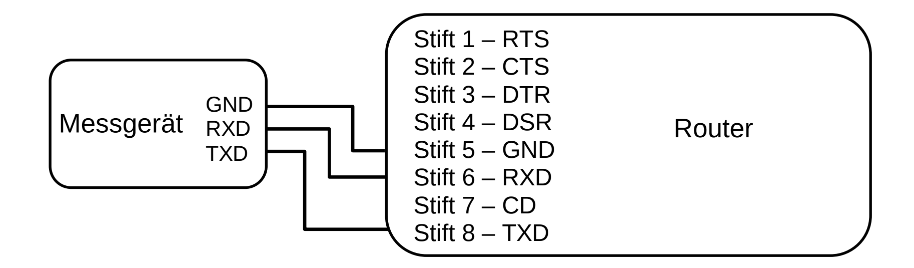
Gerätebuchse RJ45

2.8.4.1. Erweiterungsanschluss RS232

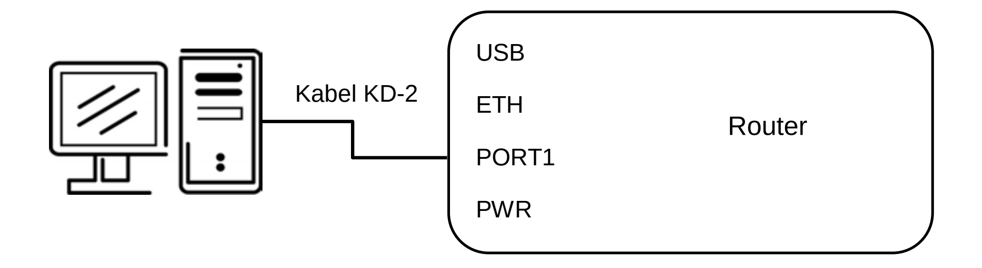
(RS232 – DCE – Data Communication Equipment)

Stiftnummer	Signalbezeichnung	Beschreibung	Datenflussrichtung
1	RTS	Request To Send	Eingang
2	CTS	Clear To Send	Ausgang
3	DTR	Data Terminal Ready	Eingang
4	DSR	Data Set Ready – auf +3,3 V über Widerstand 330 Ohm angeschlossen	Ausgang
5	GND	GROUND – Signalerde	
6	RXD	Receive Data	Ausgang
7	CD	Carrier Detect	Ausgang
8	TXD	Transmit Data	Eingang

Beispiel für den Anschluss eines Messgeräts an den Router:



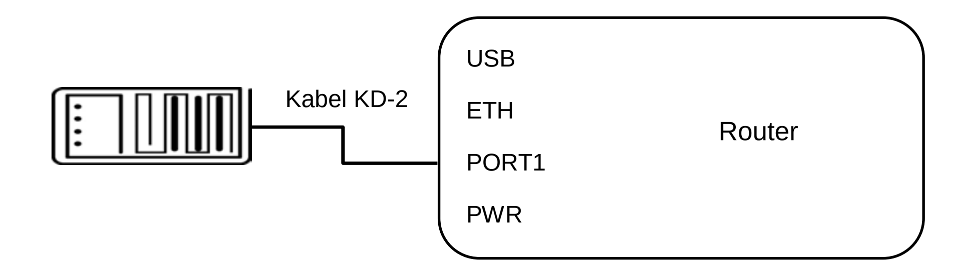
Beispiel für den Anschluss des Routers an einen PC:



- Das Kabel KD2 wird an den PC an den seriellen Anschluss (z. B. COM1) angeschlossen



Beispiel für den Anschluss des Routers an ein Gerät mit vollwertiger Schnittstelle:

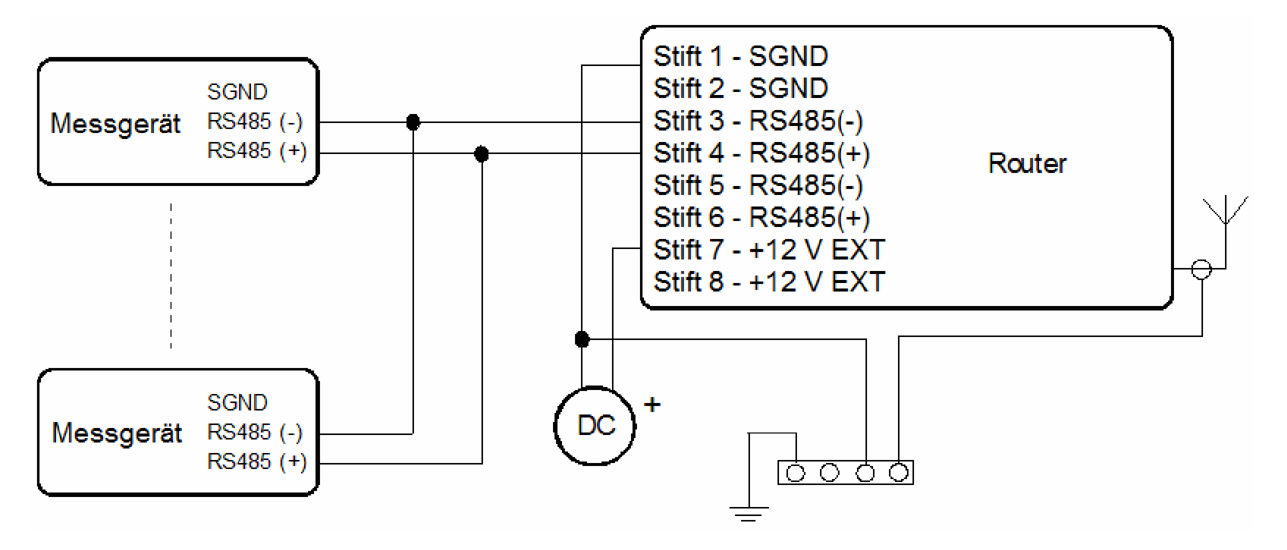


2.8.4.2. Erweiterungsanschluss RS485

Stiftnummer	Signalbezeichnung	Beschreibung	Datenflussrichtung
1	SGND	Signalerde und Erde der Stromversorgung	
2	SGND	Signalerde und Erde der Stromversorgung	
3	TxRx-	RS485 B (-)	Eingang / Ausgang
4	TxRx+	RS485 A (+)	Eingang / Ausgang
5	TxRx-	RS485 B (-)	Eingang / Ausgang
6	TxRx+	RS485 A (+)	Eingang / Ausgang
7	+12 V EXT	Externe Stromversorgung	
8	+12 V EXT	Externe Stromversorgung	

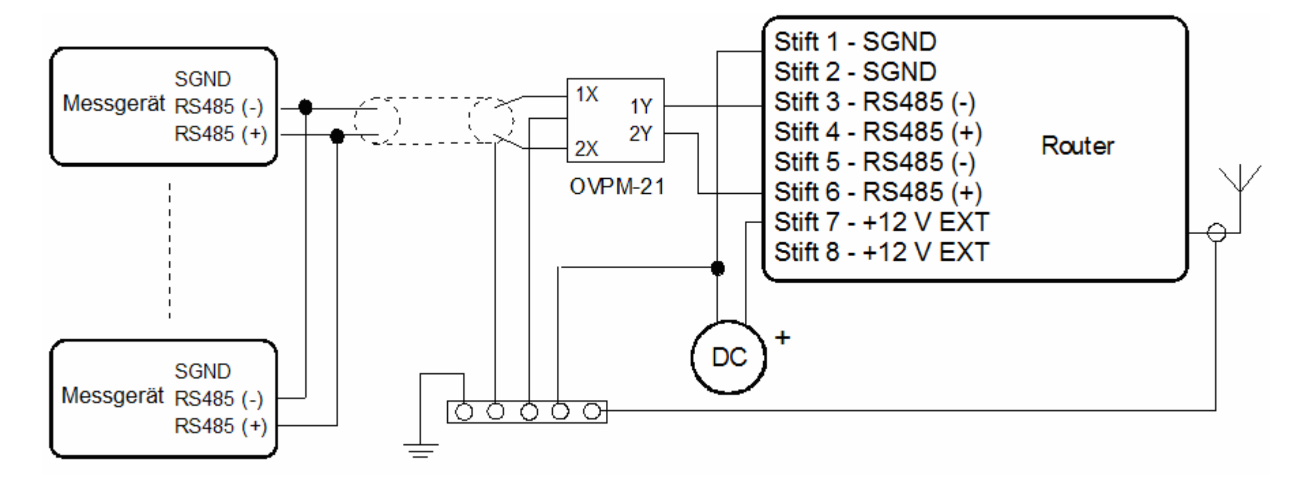
Vorsicht! Die Stromversorgung wird am Erweiterungsanschluss RS485 mit dem Brückenverbinder gewählt , siehe Kap. 2.9.
Im Bedarfsfall der galvanischen Abtrennung muss der Umwandler aus externer Stromversorgung gespeist werden.

Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels <10 m:





Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels >10 m:



Bei Länge der Datenleitung RS485 >10 m ist es notwendig, auf der Routerseite Schutzanlagen gegen Überspannung zu verwenden!

2.8.4.3. Erweiterungsanschluss RS422

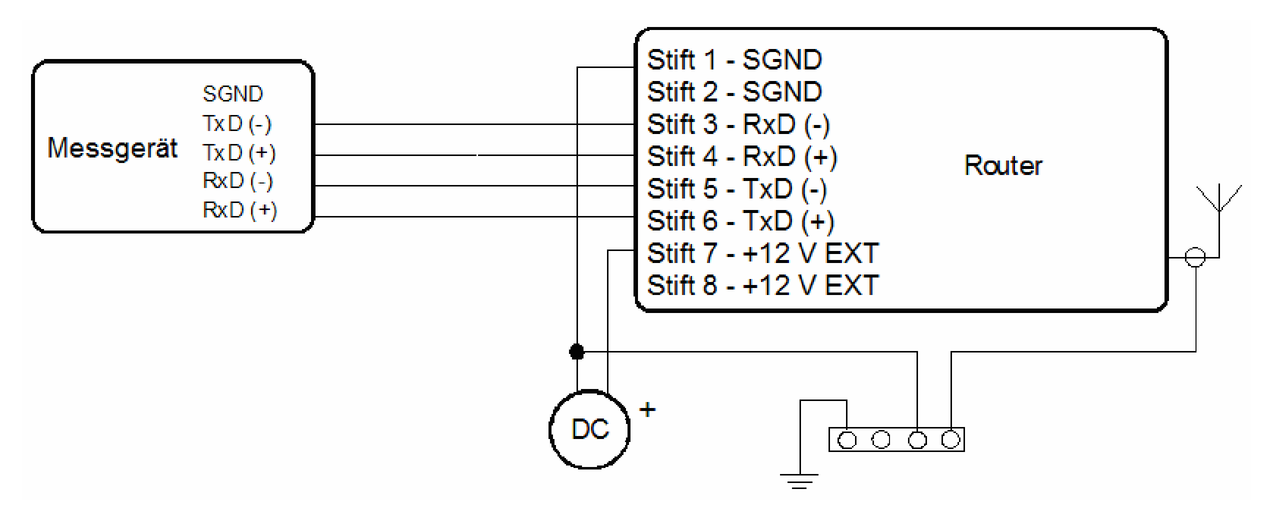
Stiftnummer	Signalbezeichnung	Beschreibung	Datenflussrichtung
1	SGND	Signalerde und Erde der Stromversorgung	
2	SGND	Signalerde und Erde der Stromversorgung	
3	RxD-	Receive data (-)	Ausgang
4	RxD+	Receive data (+)	Ausgang
5	TxD-	Transmit data (-)	Eingang
6	TxD+	Transmit data (+)	Eingang
7	+12 V EXT	Externe Stromversorgung	
8	+12 V EXT	Externe Stromversorgung	



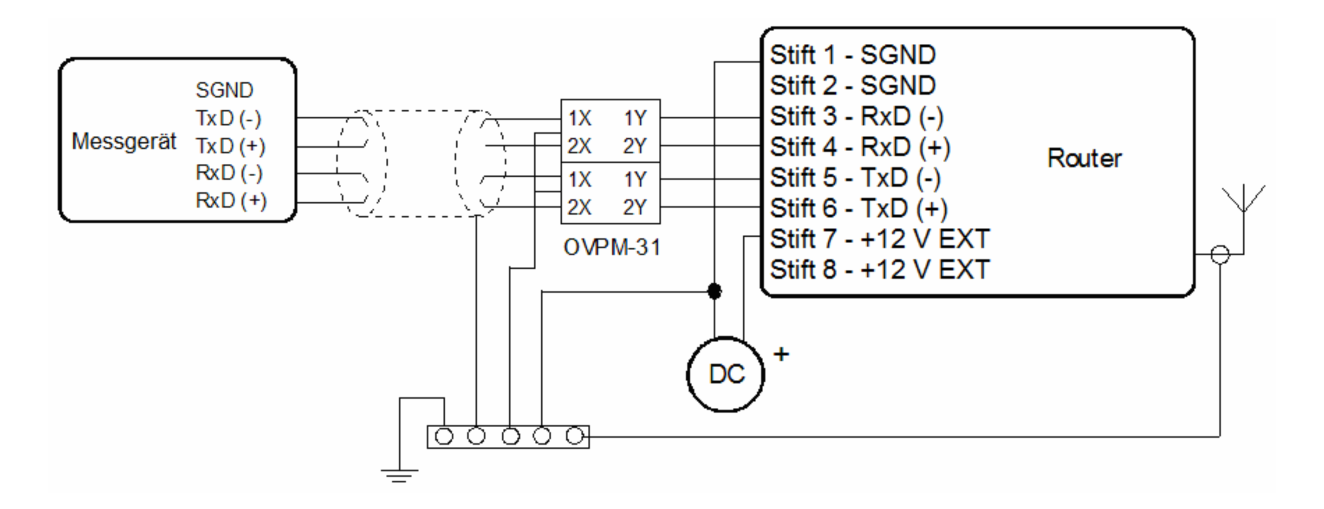
Vorsicht! Die Stromversorgung wird am Erweiterungsanschluss RS422 mit dem Brückenverbinder gewählt , siehe Kap. 2.9.

Im Bedarfsfall der galvanischen Abtrennung muss der Umwandler aus externer Stromversorgung gespeist werden.

Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels <10 m:



Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels >10 m:



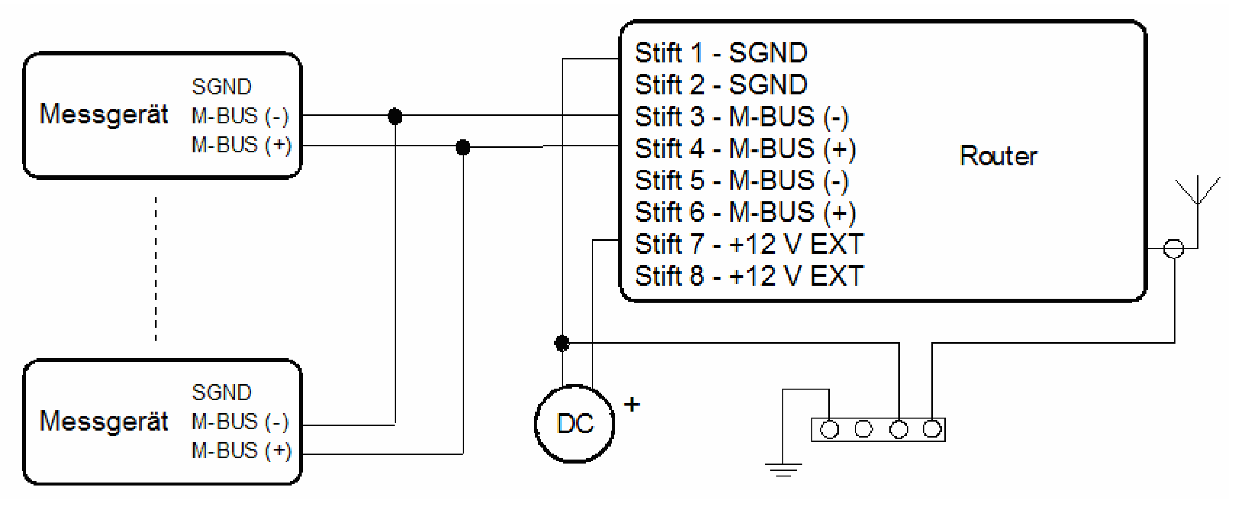
Bei Länge der Datenleitung RS422 >10 m ist es notwendig, auf der Routerseite Schutzanlagen gegen Überspannung zu verwenden!

2.8.4.4. Erweiterungsanschluss M-BUS

Stiftnummer	Signalbezeichnung	Beschreibung	Datenflussrichtung
1	SGND	Signalerde und Erde der Stromversorgung	
2	SGND	Signalerde und Erde der Stromversorgung	
3	TxRx-	MBUS B (-)	Eingang / Ausgang
4	TxRx+	MBUS A (+)	Eingang / Ausgang
5	TxRx-	MBUS B (-)	Eingang / Ausgang
6	TxRx+	MBUS A (+)	Eingang / Ausgang
7	+12 V EXT	Externe Stromversorgung	
8	+12 V EXT	Externe Stromversorgung	

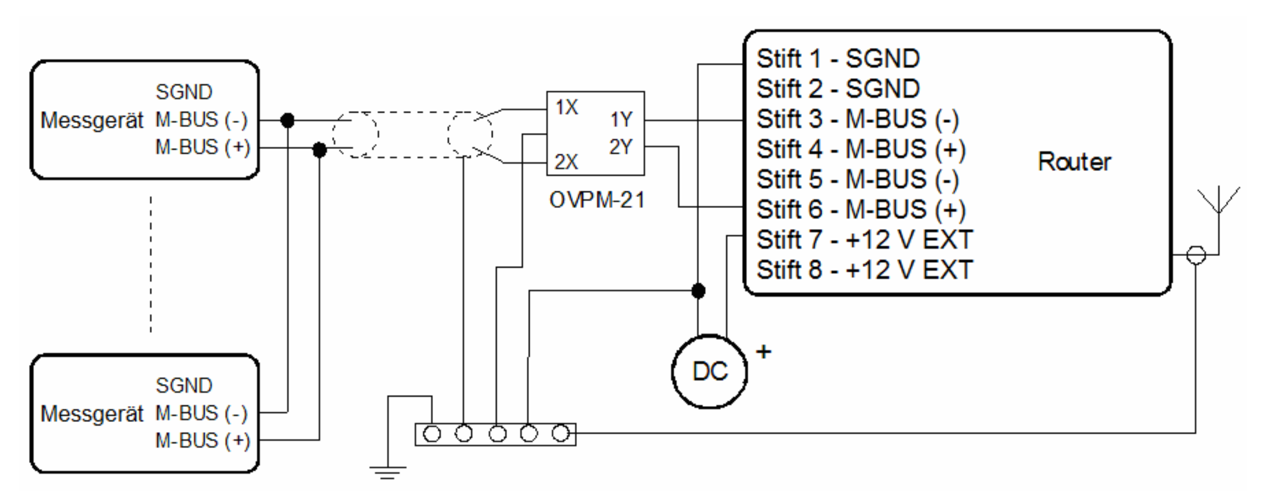
Vorsicht! Die externe Stromversorgung dient dem Erweiterungsanschluss MBUS!
Im Bedarfsfall der galvanischen Abtrennung muss der Umwandler aus externer Stromversorgung gespeist werden.

Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels <10 m:





Beispiel für den Anschluss des Messgeräts an den Router bei einer Länge des Datenkabels >10 m:





Bei der Länge der Datenleitung M-BUS >10 m ist es notwendig, auf der Routerseite Schutzanlagen gegen Überspannung zu verwenden!

2.8.4.5. Erweiterungsanschluss CNT

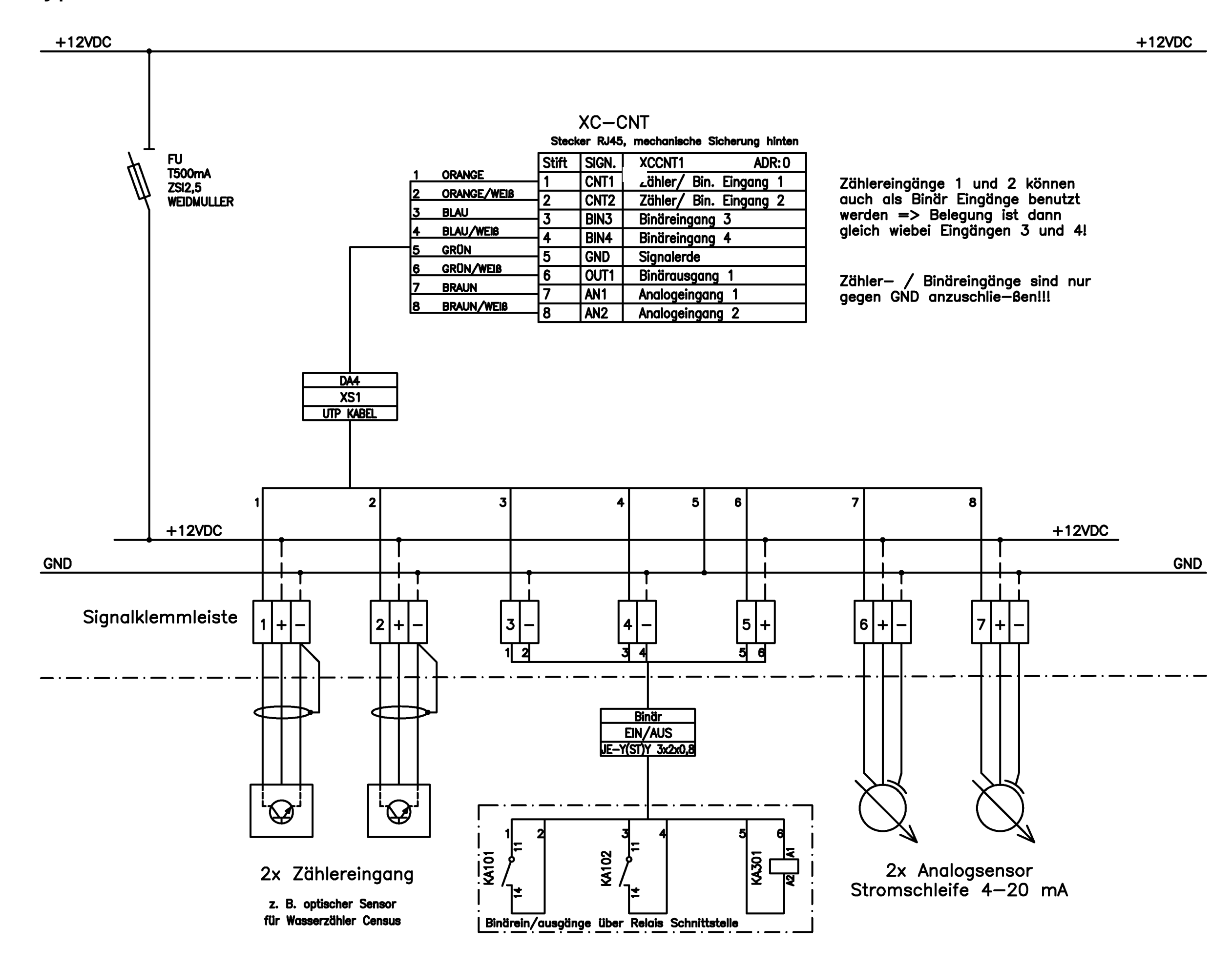
Stiftnummer	Signalbezeichnung	Beschreibung	Datenflussrichtung
1	BIN1/CNT1	Binäreingang / Zahleingang	Eingang
2	BIN2/CNT2	Binäreingang / Zahleingang	Eingang
3	BIN3	Binäreingang	Eingang
4	BIN4	Binäreingang	Eingang
5	GND	Signalerde	
6	OUT1	Binärausgang (offener Kollektor)	Ausgang
7	AN1	Analogeingang	Eingang
8	AN2	Analogeingang	Eingang

Die Benutzerschnittstelle ist zum Abgreifen und zur Bearbeitung von analogen und binären Signalen sowie zur Steuerung (Einstellung) des Binärsignals vorgesehen. Es stehen 2 Zahl- und 2 Binäreingänge oder 4 Binäreingänge, 2 Analogeingänge und 1 Binärausgang zur Verfügung Die Einstellung der Binär- und Zahleingänge erfolgt mit der Firmware, in der die einzelnen Eingänge und Ausgänge definiert werden.





Typischer Anschluss von Messkreisen:






2.9. Technische Spezifikationen des Erweiterungsanschlusses PORT1:

- Erweiterungsanschluss RS232

Expansion Port RS232		
Stromversorgung	Intern	....
Betriebsbedingungen	Betriebstemperatur	-20 bis +55 ℃
	Lagerungstemperatur	-20 bis +85 ℃
Entspricht den Normen	Emissionen	EN 55022/B
	Verträglichkeit	ETS 300 342
	Sicherheit	EN 60950
Bus RS232 (EN 1434)	Max. Belastung	15 mA
	Max. Übertragungsgeschwindigkeit	230 400 bps
	Max. Überspannung	±30 V
	Max. Kabellänge (300 Bd, 200 nF/km)	20 m

- Erweiterungsanschluss RS485-RS422

Expansion Port RS485-RS422		RS485	RS422
Stromversorgung	Extern	+10 bis +30 V	
	Intern	....	
	Leistungsaufnahme	Max. 1 W	
	Verbrauch	Max. 4 mA	
Betriebsbedingungen	Betriebstemperatur	-20 bis +55 ℃	
	Lagerungstemperatur	-20 bis +85 ℃	
Entspricht den Normen	Emissionen	EN 55022/B	
	Verträglichkeit	ETS 300 342	
	Sicherheit	EN 60950	
Bus RS485/RS422 (EN 1434)	Max. Geräteanzahl (je 1,5 mA)	256	
	Max. Übertragungsgeschwindigkeit	38400 bps	
	Kurzschlussfestigkeit	dauerhaft	
	Max. Kabellänge (300 Bd, 200 nF/km)	1200 m	

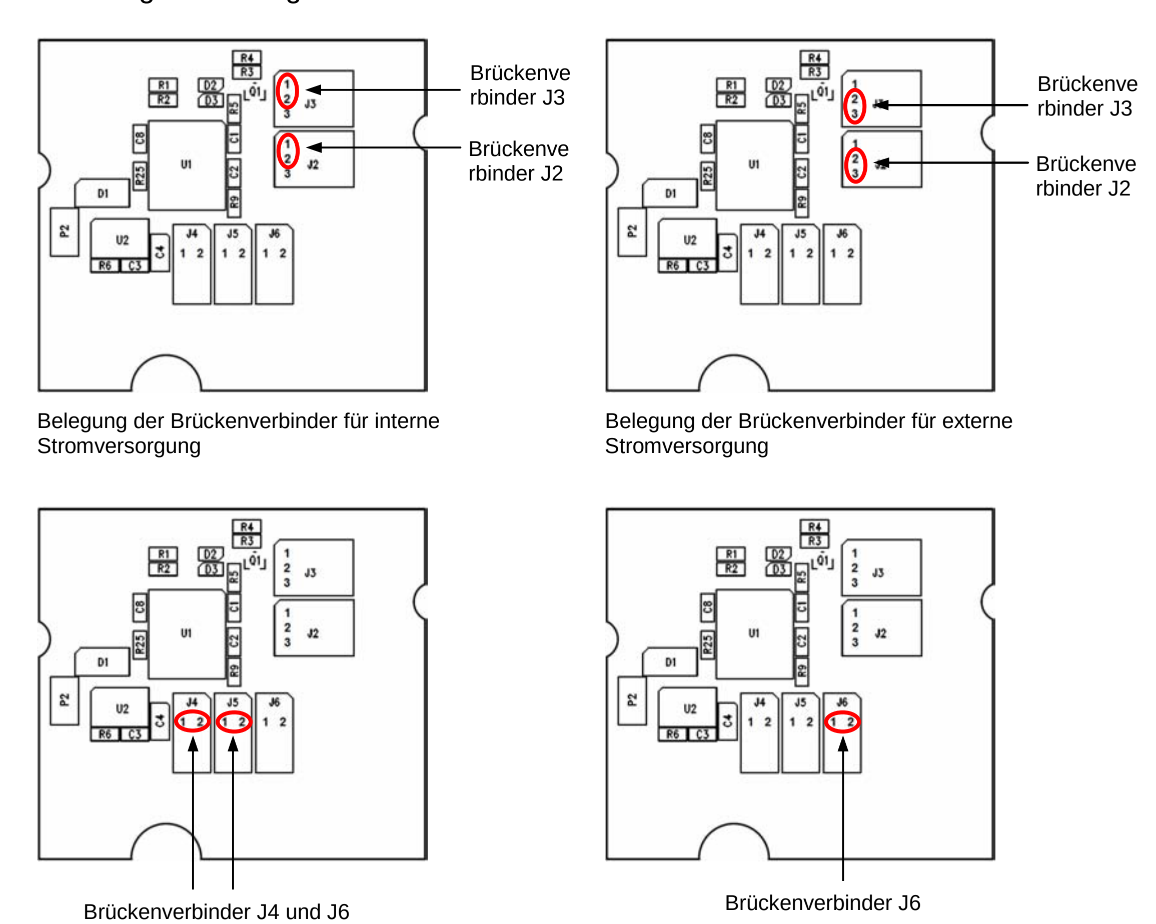


Externe oder interne Stromversorgung des Moduls Expansion Port RS485/RS422 kann durch den Anschluss der Brückenverbinder J2 und J3 an dieses Modul gewählt werden. Ist die externe Stromversorgung des Moduls erwünscht, müssen die Stifte 2–3 mit dem Brückenverbinder J2 und J3 verbunden werden. Die Interne Stromversorgung wird mit der Verbindung der Stifte 1–2 mit dem Brückenverbinder J2 und J3 gewählt.

Das Verhalten der Schnittstelle RS485 oder RS422 kann durch den Anschluss der Brückenverbinder J4, J5 und J6 an dieses Modul gewählt werden. Ist das Verhalten der Schnittstelle RS485 erwünscht, müssen die Brückenverbinder J4 und J5 geschlossen und der Brückenverbinder J6 geöffnet werden. Ist das Verhalten der Schnittstelle RS422 erwünscht, müssen die Brückenverbinder J4 und J5 geöffnet und der Brückenverbinder J6 geschlossen werden.

Die örtliche Verteilung der Brückenverbinder ist auf dem unteren Bild (Modul Expansion Port RS485/RS422 von der Oberseite TOP) zu sehen. Die interne

Stromversorgung ist nur dann zu empfehlen, wenn es nicht möglich ist eine externe Stromversorgung sicherzustellen. Ist die interne Stromversorgung gewählt, ist der Umwandler RS485/RS422 galvanisch getrennt.



Belegung der Brückenverbinder für Bus RS485

Belegung des Brückenverbinder für Bus RS422

- Erweiterungsanschluss MBUS

Expansion Port MBUS		
Stromversorgung	Versorgungsspannung	+10 bis +30 V
	Leistungsaufnahme	Max. 30 W
Betriebsbedingungen	Betriebstemperatur	-20 bis +55 ℃
	Lagerungstemperatur	-20 bis +85 ℃
Entspricht den Normen	Emissionen	EN 55022/B
	Verträglichkeit	ETS 300 342
	Sicherheit	EN 60950
Bus M-Bus (EN 1434)	Max. Geräteanzahl (je 1,5 mA)	30
	Max. Leistungsaufnahme vom Bus im Betrieb	60 mA
	Erfassung der Überlastung	100 mA
	Kurzschlussfestigkeit	dauerhaft
	Busspannung Zeichen	36 bis 43 V
	Busspannung Leerzeichen	24 bis 31 V
	Max. Kabellänge (300 Bd, 200 nF/km)	1000 m

- Erweiterungsanschluss CNT

Expansion Port CNT		
Stromversorgung	Intern	...
	Passive Betriebsbereitschaft	100 µA (funktionierender Zählereingang)
	Betrieb	2 mA
Betriebsbedingungen	Betriebstemperatur	-20 bis +55 ℃
	Lagerungstemperatur	-20 bis +85 ℃
Entspricht den Normen	Emissionen	EN 55022/B
	Verträglichkeit	ETS 300 342
	Sicherheit	EN 60950
Eingänge / Ausgänge	2x Zählereingänge	Max. 100 Hz, Tastverhältnis Max. 1:10
	2x Analogeingänge	0 bis 20 mA, R_{in} 100 Ohm
	2x Binäreingänge	Potentialfreier Kontakt
	1x Ausgang (offener Kollektor)	100 mA
Sonstiges	Überspannungsfestigkeit	dauerhaft
	Passiver Modus	Gesteuert



2.10. Anzeige des Routerzustandes

Auf der Front- und Rückplatte des Routers befinden sich insgesamt vier Kontrollleuchten (LED), die über den Routerstand informieren.

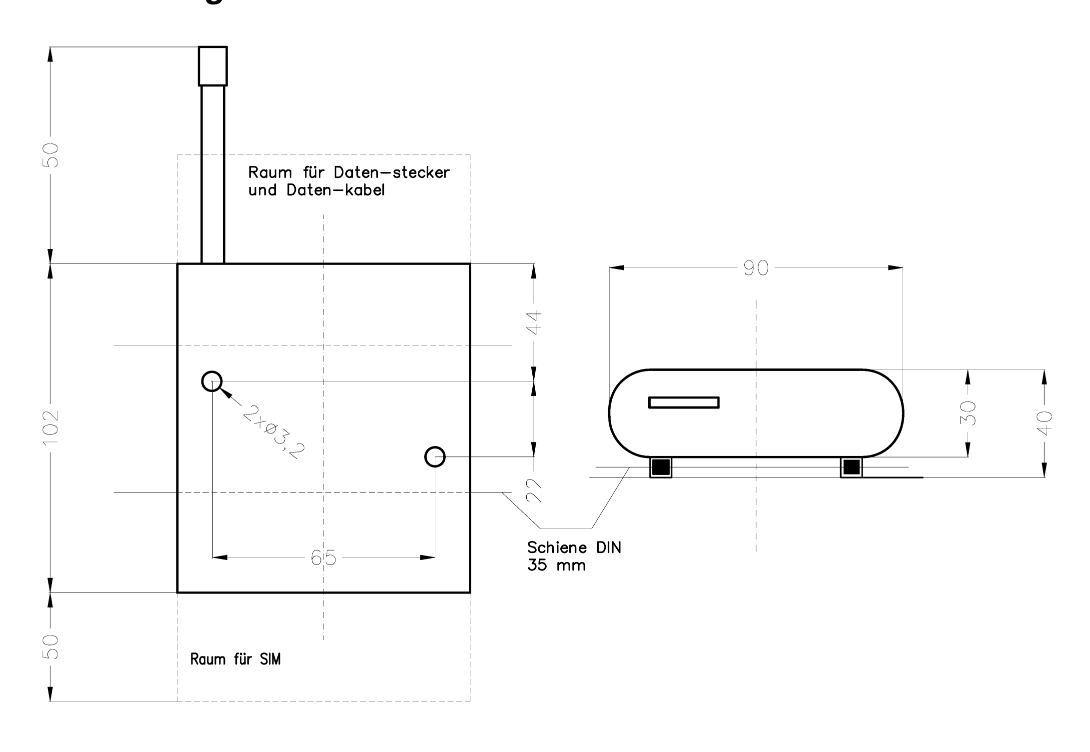
Platte	Farbe	Beschreibung	Bedeutung
Frontplatte	Grün	PWR	Sie blinkt 1:9 ……… die GPRS Verbindung wurde aufgebaut Sie blinkt 9:1 ……… die GPRS Verbindung wird aufgebaut Sie leuchtet ununterbrochen ……..das Einschalten des Routers läuft
Frontplatte	Rot	GSM	Sie blinkt ………….. die Kommunikation in GSM/GPRS läuft
Frontplatte	Gelb	SIM	Sie leuchtet unuterbrochen……... aktive zweite SIM Karte (nur bei ER 75i DUO) Sie leuchtet nicht…………………....nicht aktive zweite SIM Karte (nur bei ER 75i DUO)
Rückplatte	Grün	–	Sie leuchtet ununterbrochen ....die Ethernet-Geschwindigkeit von 100 Mbit/s gewählt Sie leuchtet nicht …………..…… die Ethernet-Geschwindigkeit von 10 Mbit/s gewählt
Rückplatte	Grün	–	Sie leuchtet ununerbrochen ………das Netzkabel ist angeschlossen Sie blinkt ……….......................…. die Datenübertragung läuft Sie leuchtet nicht …………...…… das Netzkabel ist nicht angeschlossen

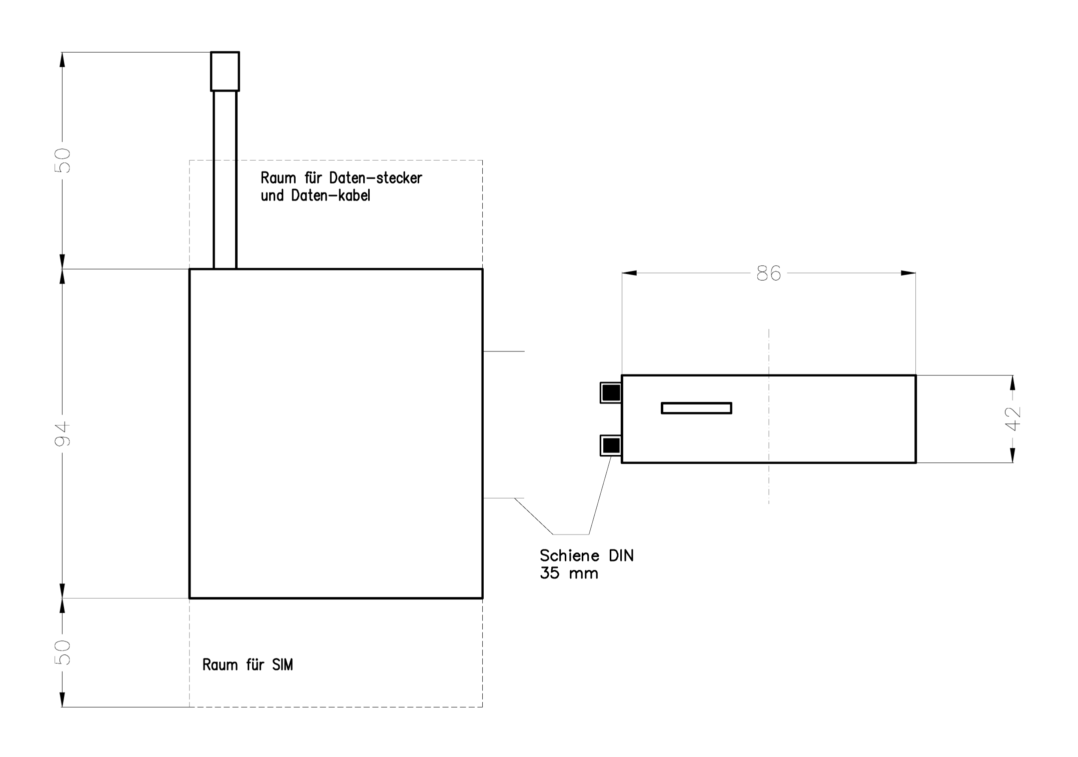
2.11. Inbetriebsetzung

Bevor Sie den Router ER 75i, ER 75i DUO oder ER 75i SL in Betrieb setzen, ist es notwendig, alle für den Lauf Ihrer Anwendungen erforderlichen Bestandteile einzuschalten, und darüber hinaus muss die SIM Karte eingelegt werden (der Router ist dabei abgeschaltet). Die SIM Karte muss GPRS unterstützen.

Der Router wird durch den Anschluss des Versorgungsnetzteils an den Router in Betrieb gesetzt. In der Ausgangseinstellung fängt der Router an, sich in das voreingestellte APN automatisch anzumelden. Das Routerverhalten kann mittels der im Folgekapitel beschriebenen Webschnittstelle geändert werden.

2.12. Mechanische und Einbauabmessungen sowie Empfehlungen zur Montage





Bei den meisten Anwendungen mit dem im Schaltschrank eingebauten Router ist es möglich, zwei Umgebungsarten zu unterscheiden:

- nicht öffentliche und industrielle Umgebung in Niederspannung mit großer Störung,
- öffentliche Stellen in Niederspannung ohne große Störung.

Für beide von diesen Umgebungen ist es möglich, die Router in den Schaltschrank einzubauen, anschließend ist es nicht notwendig, irgendwelche Beständigkeits- oder Emissionsprüfungen im Zusammenhang mit der EMV im Sinne der Norm EN 60439-1 ed.2 durchzuführen.

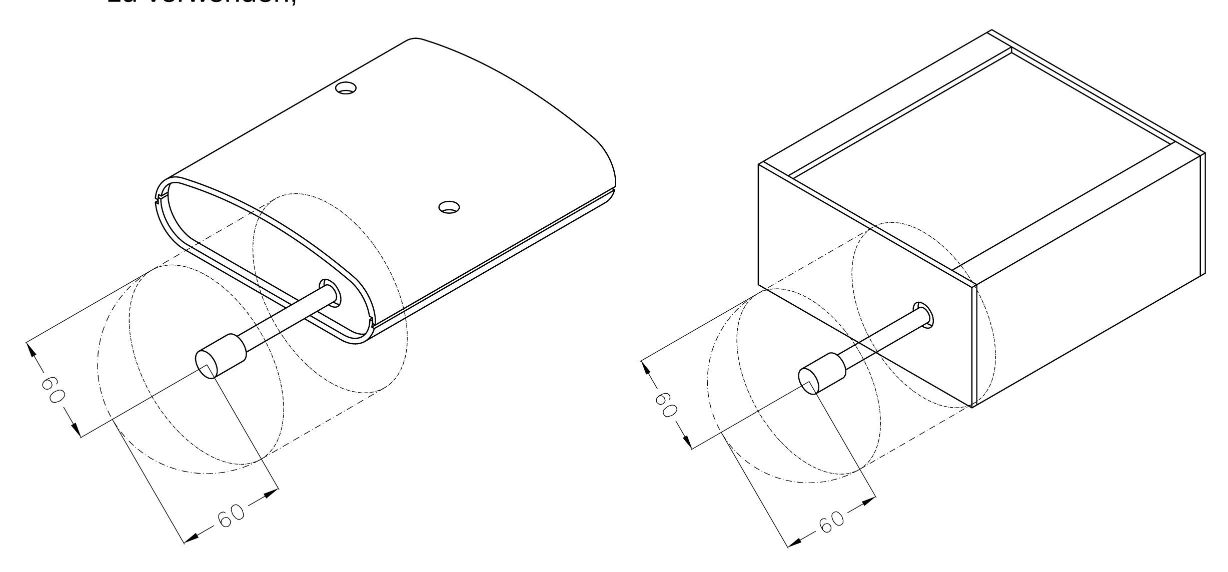
Zur Einhaltung der Norm EN 60439-1 ed.2 ist es notwendig, die folgende Montage des Routers in den Schaltschrank durchzuführen:



- es wird empfohlen, rund um die Antenne einen Abstand von 6 cm von Kabeln und Metallflächen auf jeder Seite laut dem folgenden Bild zur Vermeidung einer Störungen einzuhalten, bei der Verwendung von externen Antenne außerhalb des Schaltschrankes ist es notwendig, die geeigneten Schutzanlagen gegen Überspannung (Blitzableiter) einzusetzen,

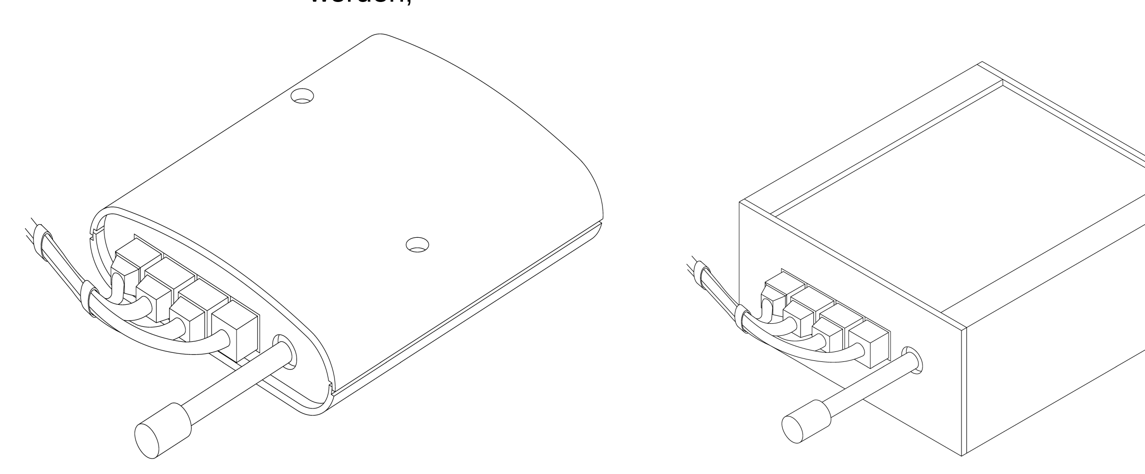


- bei der Montage des Routers auf das Stahlblech wird empfohlen eine externe Antenne zu verwenden,



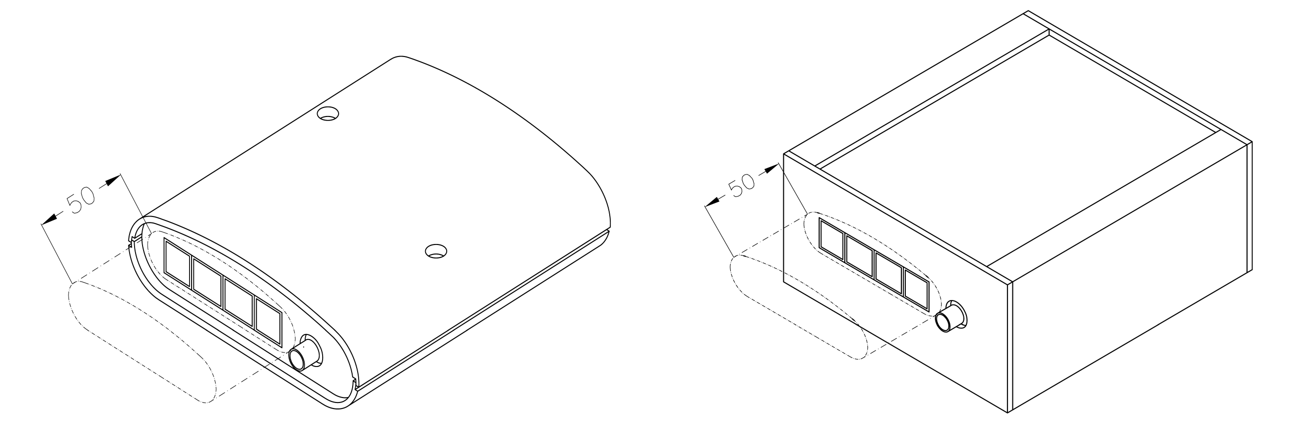


- es wird empfohlen, die einzelnen Kabel in ein Bündel (siehe Bild weiter unten) einzubinden. Für die auf diese Weise geführten Kabel gelten folgende Begrenzungen:
  - die Bündellänge (Kombination der Stromversorgungs- und Datenkabel) kann maximal 1,5 m betragen, überschreitet die Länge der Datenkabel 1,5 m oder im Falle, dass die Datenkabel außerhalb des Schaltschrankes geführt werden, wird empfohlen, eine geeigneten Schutzanlagen gegen Überspannung (Blitzableiter) zu verwenden,
  - zusammen mit den Datenkabeln dürfen nicht die Kabel, die Netzspannung ~ 230 V/50 Hz übertragen, geführt werden,
  - die Signale zu den Sensoren müssen mit den verdrillten Paaren geführt werden,





- vor den einzelnen Steckverbindern muss ein gewisser Abstand zur Handhabung der Kabel beim etwaigen Anschließen und Abtrennen der einzelnen Kabel bestehen bleiben,

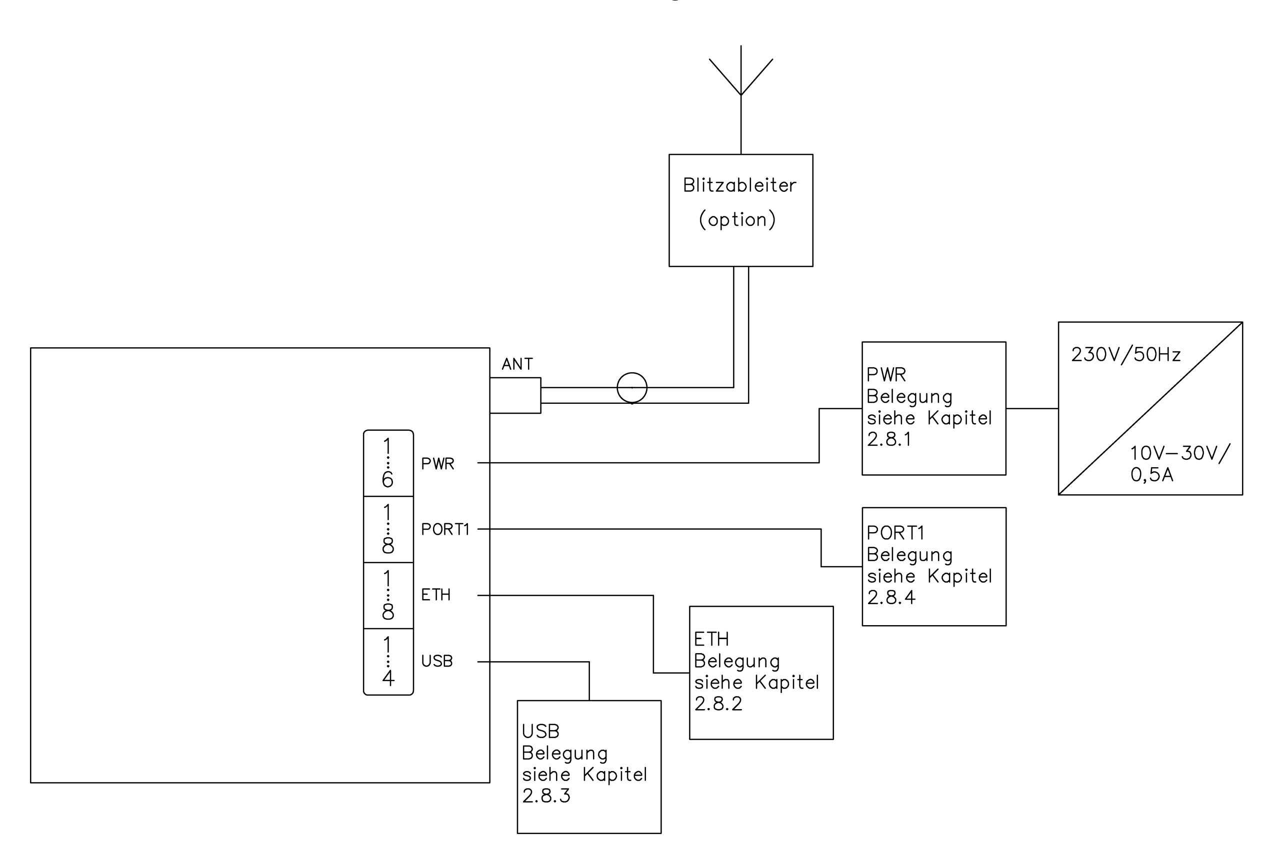




- für die richtige Funktion des Routers wird empfohlen, im Schaltschrank die Erdungsklemmleiste zur Erdung des Versorgungsnetzteils für das Modem, das Datenkabel und die Antenne zu verwenden,



- der Anschluss des Routers ist aus dem folgenden Bild ersichtlich.

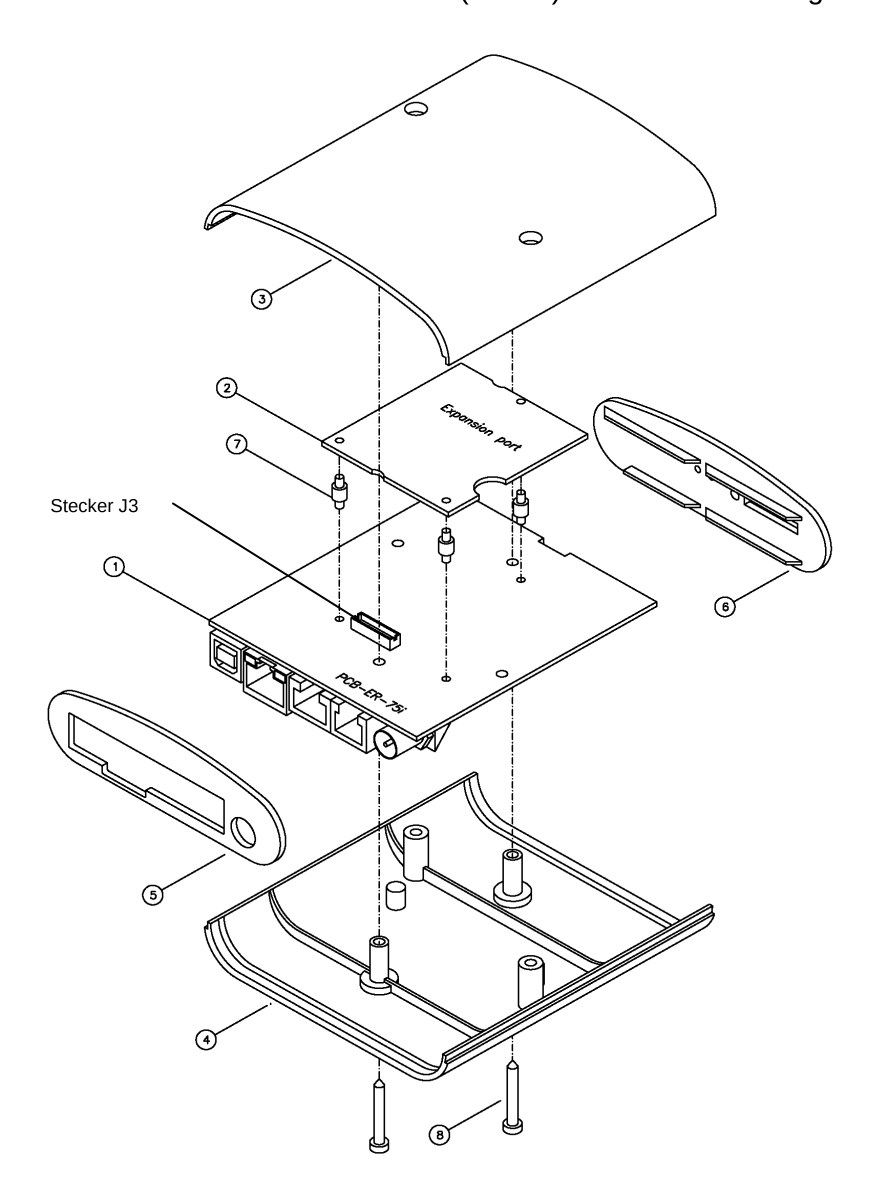


3. Einsatz des Erweiterungsanschlusses

3.1. Einsatz des Erweiterungsanschlusses des Routers ER 75i a ER 75i DUO

Vorsicht! Der Erweiterungsanschluss wird angeschlossen, während der Router abgeschaltet ist.

Nach dem Abschrauben von zwei Schrauben (Pos. 8) am unteren Gehäuseteil (Pos. 4) und nach dem Abnehmen des oberen Gehäuseteils (Pos. 3) wird der Erweiterungsanschluss (Pos. 2) in den Steckverbinder J3 (siehe Bild unten) der Grundplatte des Routers B-ER-75i (Pos. 1) von der TOP Seite angeschlossen. Der Erweiterungsanschluss wird zur Grundplatte des Routers mit 3 Stück Abstand haltender Säulen (Pos. 7) befestigt. Nach dem Aufsetzen des Anschlusses wird das Gehäuse mit Schrauben (Pos. 8) wieder zusammengeschraubt.



Liste und Beschreibung der Teile

Teil	Beschreibung	Anzahl
11	Grundplatte des EDGE Routers	1
2	Erweiterungsanschluss PORT1	1
3	Oberer Gehäuseteil	1
4	Unterer Gehäuseteil	1
5	Hinterer Frontteil	1
6	Vorderer Frontteil	1
7	Abstand haltende Säule zur Befestigung des Erweiterungsanschlusses zur Grundplatte	3
8	Schraube zur Fertigstellung des Gehäuses	2

3.2. Einsatz des Erweiterungsanschlusses des Routers ER 75i SL



Vorsicht! Der Erweiterungsanschluss wird angeschlossen, während der Router ER 75i SL abgeschaltet ist.

Nach dem Abschrauben von vier Schrauben (Pos. 10) am hinteren Frontteil des Gehäuses (Pos. 5) und nach dem Abnehmen ist es möglich, die Platte ER-75i (Pos. 1) herauszuschieben. Der Erweiterungsanschluss (Pos. 2) wird in den Steckverbinder J3 (unteres Bild) der Grundplatte des Routers B-ER-75i (Pos. 1) von der TOP Seite angeschlossen. Der Erweiterungsanschluss wird zur Grundplatte des Routers mit 3 Stück Abstand haltender Säulen (Pos. 9) befestigt. Nach dem Aufsetzen des Anschlusses wird das Gehäuse mit Schrauben (Pos. 10) wieder zusammengeschraubt.

Stecker J3

Liste und Beschreibung der Teile

Teil	Beschreibung	Anzahl
11	Grundplatte des EDGE Routers	1
2	Erweiterungsanschluss PORT1	1
3	Linke Seitenwand des Routers	1
4	Rechte Seitenwand des Routers	1
5	Hinterer Frontteil des Routers	1
6	Vorderer Frontteil des Routers	1
7	Unterer Gehäuseteil des Routers	1
8	Oberer Gehäuseteil des Routers	1
9	Abstand haltende Säule zur Befestigung des Erweiterungsanschlusses zur Grundplatte	3
10	Schraube zur Fertigstellung des Gehäuses	8

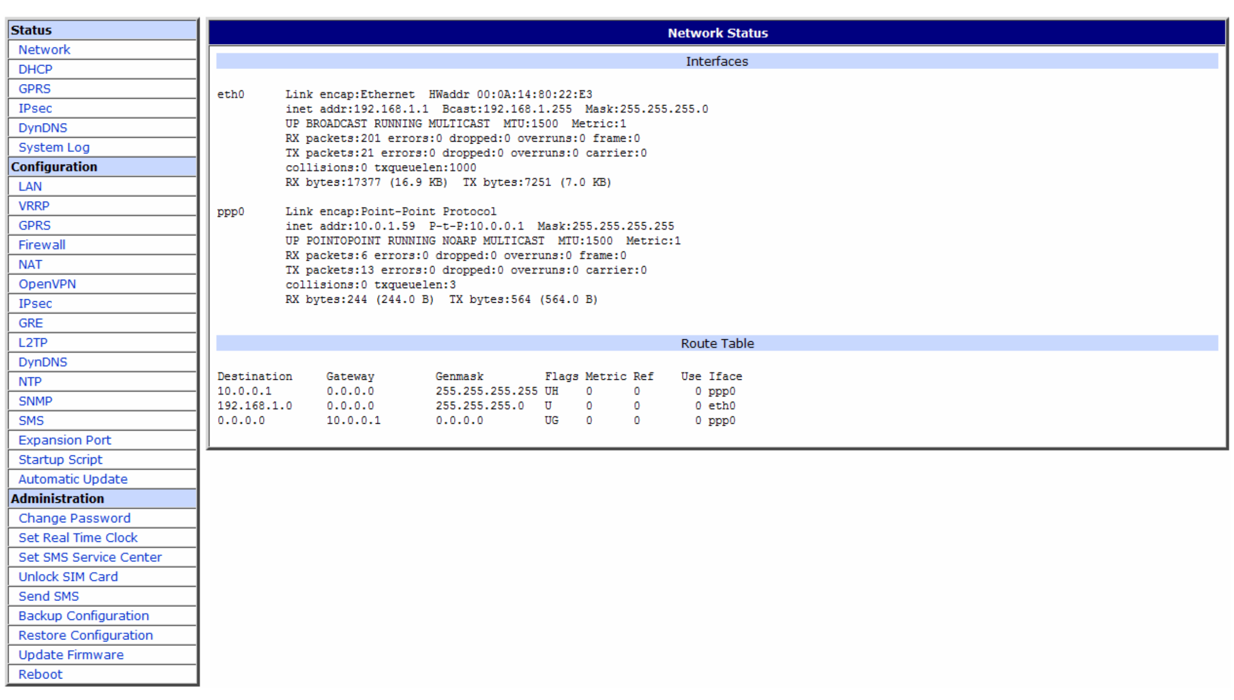
4. Einstellung der Konfiguration über den Webbrowser



Vorsicht! Ohne eingelegte SIM Karte kann der Router nicht betrieben werden. Die eingelegte SIM Karte muss die GPRS Übertragungen aktiviert haben. Die SIM Karte legen Sie nur dann ein, wenn der Router abgeschaltet ist.

Zur Zustandsüberwachung, Konfiguration und Verwaltung des Routers steht eine Webschnittstelle zur Verfügung. Diese kann durch die Eingabe der IP Adresse des Routers in den Webbrowser aufgerufen werden. Die IP Ausgangsadresse des Routers lautet 192.168.1.1. Die Konfiguration kann nur der Benutzer „root” mit dem Ausgangspasswort „root” vornehmen.

Im linken Teil der Webschnittstelle ist das Menü mit der Optionsauswahl der Seiten zur Überwachung des Zustandes (Status), zur Konfiguration (Configuration) und zur Verwaltung (Administration) des Routers untergebracht.



Nachdem die LED Diode PWR auf der Fronttafel anfängt zu blinken, ist es möglich, die Ausgangseinstellung des Routers durch die Betätigung der RST Taste wiederherzustellen, damit wird die Wiederherstellung der Konfiguration und das anschließende Reset/Zurücksetzen vorgenommen (grüne LED Diode leuchtet auf).

4.1. Netzinformationen

Die Netzinformationen über den Betrieb des Routers können durch die Auswahl der Option *Network* im Menü aufgerufen werden. Im unteren Fensterteil wird die Information über die Richttabelle angezeigt. Im oberen Fensterteil werden ausführliche Informationen über die aktiven Schnittstellen angezeigt.

- eth0 – Netzschnittstelle
- ppp0 – PPP Schnittstelle (aktiver Anschluss in GPRS/EDGE)
- tun0 – Schnittstelle des OpenVPN Tunnels
- ipsec0 – Schnittstelle des IPsec Tunnels
- gre1 – Schnittstelle des GRE Tunnels

Bei jeder Schnittstelle werden dann folgende Informationen angezeigt:

- HWaddr – (einzigartige) Hardwareadresse der Netzschnittstelle
- inet – eigene IP Adresse
- P-t-P – IP Adresse des gegenüber liegenden Endes der Verbindung
- Bcast – Sendungsadresse
- Mask – Netzmaske
- MTU – maximale Paketgröße, für die das Element das Übertragungsvermögen hat
- Metric – Anzahl der Router, über die das Paket durchgehen muss
- RX packets – empfangene Pakete, Errors – Fehler, Dropped – ausgelassene Pakete
- TX packets – abgesandte Pakete, Errors – Fehler, Dropped – ausgelassene Pakete
- Collisions – Kollisionen
- RX bytes – Gesamtanzahl der empfangenen Bytes
- TX bytes – Gesamtanzahl der abgesandten Bytes

Aus den Netzinformationen ist der Zustand der GPRS Verbindung ersichtlich. Ist die GPRS Verbindung aktiv, wird in den Systeminformationen die ppp0 Verbindung angezeigt.

Network Status

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 00:CF:52:08:CF:01
          inet addr:192.168.2.254  Bcast:192.168.2.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:336 errors:0 dropped:0 overruns:0 frame:0
          TX packets:101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32435 (31.6 KB)  TX bytes:50905 (49.7 KB)

gre1      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:192.168.2.254  P-t-P:192.168.2.254  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1476  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

ipsec0    Link encap:Point-Point Protocol
          inet addr:10.0.2.38  Mask:255.255.255.255
          UP RUNNING NOARP  MTU:16260  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:10
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

ppp0      Link encap:Point-Point Protocol
          inet addr:10.0.2.38  P-t-P:10.0.0.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:314 (314.0 B)  TX bytes:678 (678.0 B)
```

Route Table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.1        0.0.0.0         255.255.255.255 UH    0      0        0 ppp0
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 gre1
0.0.0.0         10.0.0.1        0.0.0.0         UG    0      0        0 ppp0
```

4.2. DHCP Status

Die Informationen über die vom DHCP Server dem Router zugeteilten IP Adressen sind im Menü in der Option *DHCP zu finden:*

- lease 192.168.1.2 (im allgemeinen IP Adresse) – zugeteilte IP Adresse
- starts – die Zeit der Zuteilung der IP Adresse
- ends – Dauer der Gültigkeit der zugeteilten IP Adresse
- hardware ethernet – (einzigartige) Hardwareadresse MAC
- uid – einzigartige ID Nummer

DHCP Status

Active DHCP Leases

```
lease 192.168.1.2 {
        starts 4 1970/01/01 00:00:18;
        ends 4 1970/01/01 00:10:18;
        hardware ethernet 00:40:f4:8a:5c:76;
        uid 01:00:40:f4:8a:5c:76;
}
```

Im Grenzfall kann der DHCP Status zu einer IP Adresse mehrere Eintragungen anzeigen, die Ursache dafür kann das Zurücksetzen der Netzkarte sein.

4.3. IPsec Status

Die Informationen über den aktuellen Zustand des IPsec Tunnels können durch die Auswahl der Option IPsec im Menü aufgerufen werden. Die genaue Beschreibung der hier angezeigten Informationen finden Sie auf http://www.freeswan.org/doc.html.

IPsec Status

IPsec Tunnel Info

```
000 interface ipsec0/ppp0 10.0.2.38
000
000 "ipsec": 10.0.2.38...10.0.2.39
000 "ipsec":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
000 "ipsec":   policy: PSK+ENCRYPT+TUNNEL; interface: ppp0; unrouted
000 "ipsec":   newest ISAKMP SA: #0; newest IPsec SA: #0; eroute owner: #0
000 "ipsec":   IKE algorithms wanted: 5_000-1-5, 5_000-2-5, 5_000-1-2, 5_000-2-2, flags=-strict
000 "ipsec":   IKE algorithms found:  5_192-1_128-5, 5_192-2_160-5, 5_192-1_128-2, 5_192-2_160-2,
000 "ipsec":   ESP algorithms wanted: 3_000-1, 3_000-2, flags=-strict
000 "ipsec":   ESP algorithms loaded: 3/168-1/128, 3/168-2/160,
000
000 #1: "ipsec" STATE_MAIN_I1 (sent MI1, expecting MR1); born:0s; EVENT_RETRANSMIT in 13s
```

4.4. GPRS Status

Die Option GPRS im Menü enthält die aktuellen Informationen über PLMN (Code des Netzbetreibers), über die Zelle, den Kanal und die Signalqualität der ausgewählten Zelle sowie der anliegenden vernehmbaren Zellen. Im unteren Teil dieses Fensters werden die Informationen über den Aufbau der GPRS/EDGE Verbindung und über etwaige Probleme bei der Herstellung dieser Verbindung angezeigt (PPP Connection Log).

GPRS Status

Actual GSM Info

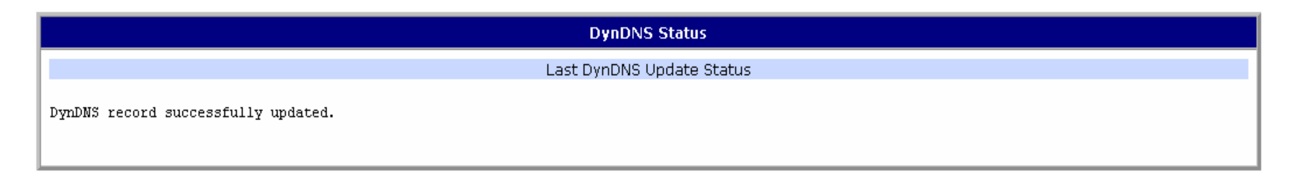
```
PLMN       : 23001
Cell       : 69A6 (EDGE attached)
Channel    : 30
Level      : -70 dBm
Neighbours : -76 dBm (80), -90 dBm (57), -92 dBm (55), -96 dBm (76), -96 dBm (59)
```

PPP Connection Log

```
1999-11-30 00:00:24 Connection successfully established.
```

4.5. DynDNS Status

Das Ergebnis der Aktualisierung der DynDNS Aufzeichnung am Server www.dyndns.org kann durch Auswahl der Option DynDNS im Menü aufgerufen werden.



DynDNS Status

Last DynDNS Update Status

DynDNS record successfully updated.

4.6. System Log

Bei Problemen mit dem Aufbau der Verbindung in GPRS oder mit dem Aufbau des IPsec Tunnels kann System Log durch Auswahl der Option *System Log* im Menü aufgerufen werden. System Log überwacht nur den Aufbau der Verbindung in GPRS und die Herstellung des IPsec Tunnels. Log Dämon kann mit der Betätigung der *Stopp* Taste eingestellt werden. Der Neustart ist mit der Betätigung der *Start* Taste möglich. Im unteren Teil des Fensters werden die ausführlichen Meldungen der einzelnen im Router laufenden Anwendungen angezeigt. Der Fensterinhalt kann durch die Betätigung der *Refresh* Taste aktualisiert werden. Mit der Save Taste *ist es möglich, System Log im Computer zu speichern.*

System Log

System Messages

```
1999-11-30 00:01:52 pppd[182]: rcvd [LCP EchoRep id=0x3 magic=0x2df617d0]
1999-11-30 00:02:22 pppd[182]: sent [LCP EchoReq id=0x4 magic=0x52fb0480]
1999-11-30 00:02:22 pppd[182]: rcvd [LCP EchoRep id=0x4 magic=0x2df617d0]
1999-11-30 00:02:52 pppd[182]: sent [LCP EchoReq id=0x5 magic=0x52fb0480]
1999-11-30 00:02:52 pppd[182]: rcvd [LCP EchoRep id=0x5 magic=0x2df617d0]
1999-11-30 00:03:22 pppd[182]: sent [LCP EchoReq id=0x6 magic=0x52fb0480]
1999-11-30 00:03:22 pppd[182]: rcvd [LCP EchoRep id=0x6 magic=0x2df617d0]
1999-11-30 00:03:52 pppd[182]: sent [LCP EchoReq id=0x7 magic=0x52fb0480]
1999-11-30 00:03:52 pppd[182]: rcvd [LCP EchoRep id=0x7 magic=0x2df617d0]
1999-11-30 00:04:22 pppd[182]: sent [LCP EchoReq id=0x8 magic=0x52fb0480]
1999-11-30 00:04:22 pppd[182]: rcvd [LCP EchoRep id=0x8 magic=0x2df617d0]
1999-11-30 00:04:52 pppd[182]: sent [LCP EchoReq id=0x9 magic=0x52fb0480]
1999-11-30 00:04:52 pppd[182]: rcvd [LCP EchoRep id=0x9 magic=0x2df617d0]
1999-11-30 00:05:22 pppd[182]: sent [LCP EchoReq id=0xa magic=0x52fb0480]
1999-11-30 00:05:22 pppd[182]: rcvd [LCP EchoRep id=0xa magic=0x2df617d0]
1999-11-30 00:05:52 pppd[182]: sent [LCP EchoReq id=0xb magic=0x52fb0480]
1999-11-30 00:05:52 pppd[182]: rcvd [LCP EchoRep id=0xb magic=0x2df617d0]
1999-11-30 00:06:22 pppd[182]: sent [LCP EchoReq id=0xc magic=0x52fb0480]
1999-11-30 00:06:22 pppd[182]: rcvd [LCP EchoRep id=0xc magic=0x2df617d0]
1999-11-30 00:06:52 pppd[182]: sent [LCP EchoReq id=0xd magic=0x52fb0480]
1999-11-30 00:06:52 pppd[182]: rcvd [LCP EchoRep id=0xd magic=0x2df617d0]
1999-11-30 00:07:22 pppd[182]: sent [LCP EchoReq id=0xe magic=0x52fb0480]
1999-11-30 00:07:22 pppd[182]: rcvd [LCP EchoRep id=0xe magic=0x2df617d0]
1999-11-30 00:07:52 pppd[182]: sent [LCP EchoReq id=0xf magic=0x52fb0480]
1999-11-30 00:07:52 pppd[182]: rcvd [LCP EchoRep id=0xf magic=0x2df617d0]
```

Stop | Refresh | Save

4.7. Konfiguration der Netzschnittstelle

Die Konfiguration der Netzschnittstelle kann durch Auswahl der Option LAN im Menü aufgerufen werden. Im ersten Fensterteil können die eigene IP Adresse der Netzschnittstelle (*IP Address*), die Netzmaske (*Subnet Mask*) und der Mediumtyp (*Media type*) definiert werden, in den meisten Fällen funktioniert *Auto-Negotiation*.

Im zweiten Fensterteil kann der DHCP Server durch das Ankreuzen der Option *Enable dynamic DHCP leases* freigegeben werden. Im Fenster kann der Anfang (*IP Pool Start*) und das Ende (*IP Pool End*) des Bereichs von IP Adressen, die den DHCP Klienten zugeteilt werden, definiert werden. Wird die Option *Enable dynamic DHCP leases* nicht angekreuzt, teilt der Router die IP Adressen nicht zu.

Im dritten Fensterteil ist es möglich, durch das Ankreuzen der Option *Enable static DHCP leases* die Zuteilung von bis zu vier statischen IP Adressen (*IP Address*), die den MAC Adressen (*MAC Address*) der angeschlossenen Geräte, Stationen usw. entsprechen, zu definieren.

Die Änderungen der Einstellung wirken sich nach der Betätigung der Apply Taste aus.

Der DHCP Server teilt den angeschlossenen Kunden die IP Adressen des definierten Adressenbereiches, die IP Gatewayadresse und IP Adresse des DNS Servers zu. Es ist wichtig, dass sich die Bereiche der statisch vorgegebenen IP Adressen und der vom DHCP zugeteilten Adressen nicht überlappen, ansonsten kann eine Adressenkollision und somit eine falsche Netzfunktion auftreten.

LAN Configuration

IP Address 192.168.1.1
Subnet Mask 255.255.255.0
Media Type Auto-Negotiation

☐ Enable dynamic DHCP leases
IP Pool Start 192.168.1.2
IP Pool End 192.168.1.254

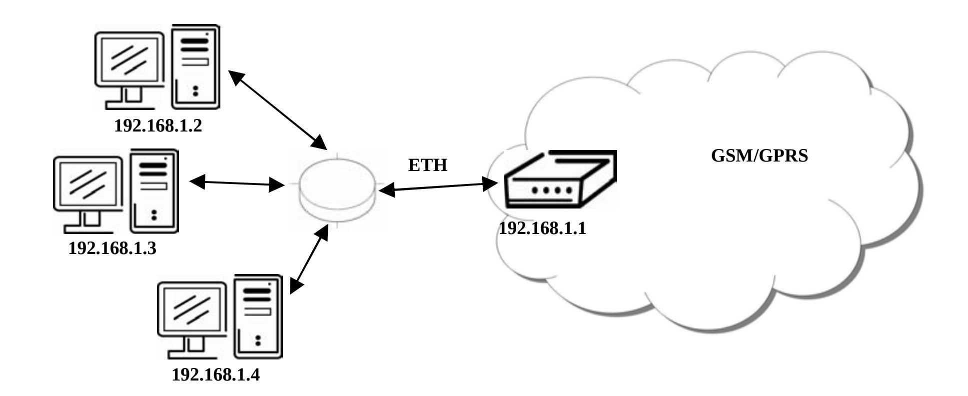
☐ Enable static DHCP leases

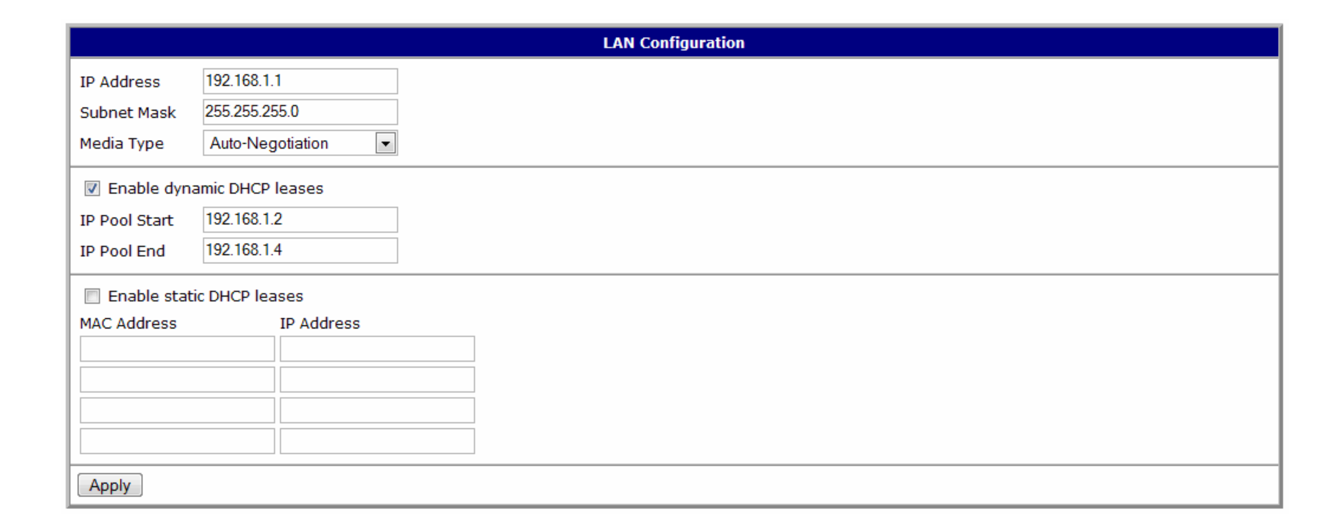
MAC Address	IP Address

Apply

LUCOM GmbH * Ansbacher Str. 2a * 90513 Zirndorf * Tel. 09127/59 460-10 * Fax. 09127/59 460-20 * www.lucom.de

Beispiel für die Einstellung der Netzschnittstelle mit dynamischem DHCP Server:





LAN Configuration

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Media Type	Auto-Negotiation

☑ Enable dynamic DHCP leases

IP Pool Start	192.168.1.2
IP Pool End	192.168.1.4

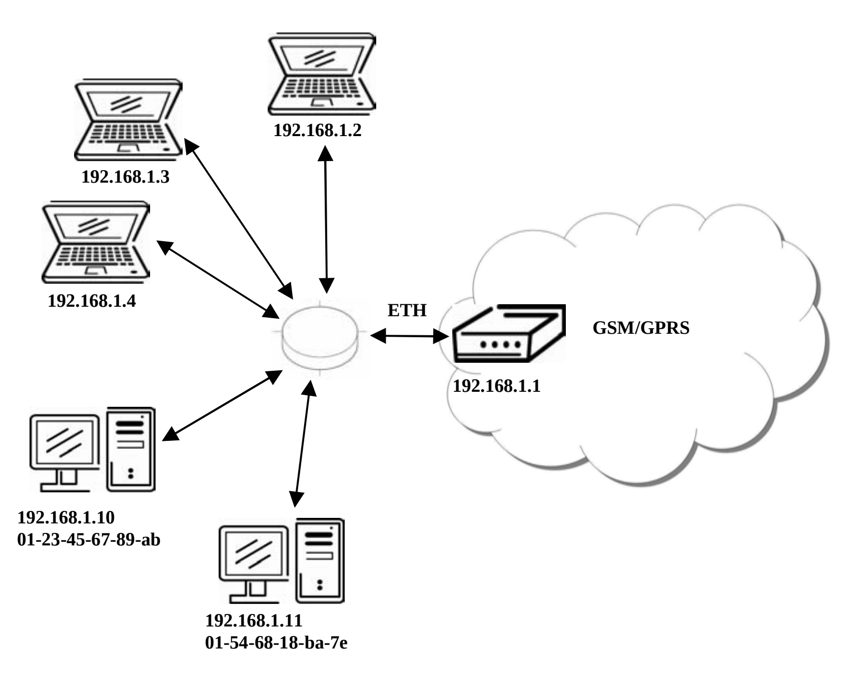
☐ Enable static DHCP leases

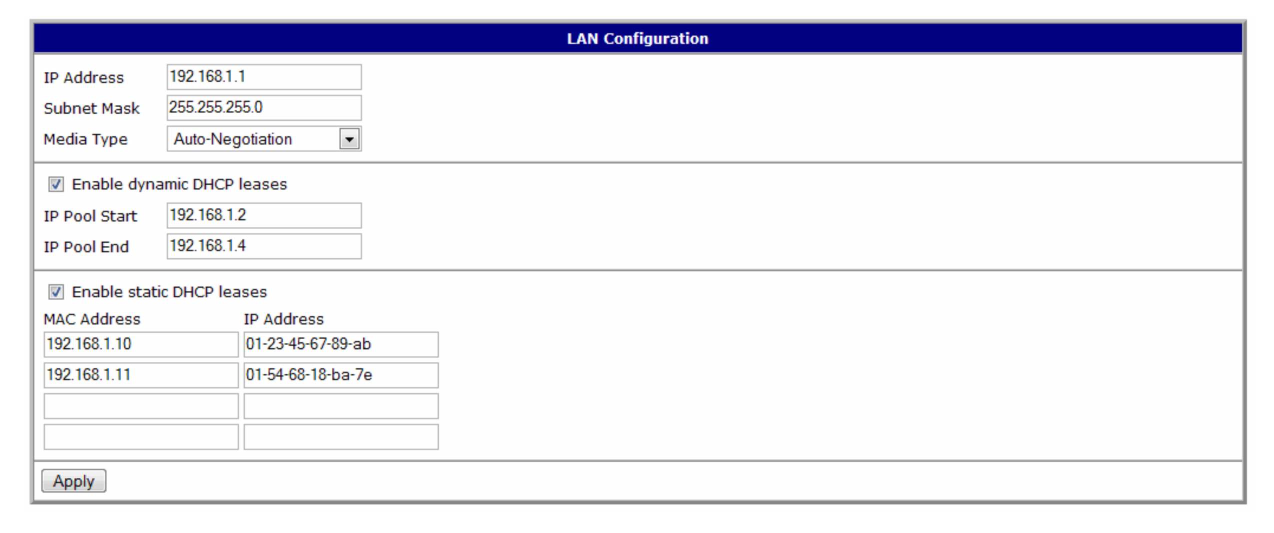
MAC Address	IP Address

Apply



Beispiel für die Einstellung der Netzschnittstelle mit dem dynamischen und statischen DHCP Server:





4.8. VRRP Konfiguration

Die VRRP Konfiguration kann durch die Auswahl der Option VRRP im Menü aufgerufen werden. Das Protokoll VRRP (Virtual Router Redundancy Protocol) ist eine Technik, mittels der es möglich ist, die Richtpflichten von einem Hauptrouter auf einen anderen Reserverouter zu übertragen, falls der Hauptrouter versagt. Das Protokoll VRRP kann durch das Ankreuzen der Option *Enable VRRP* freigegeben werden. Der Parameter *Virtual Server IP Address* stellt die IP Adresse des virtuellen Servers ein, diese Adresse ist für beide Router gleich. Das angeschlossene Gerät sendet seine Daten über diese virtuelle Adresse. Sollten im Netz mehrere virtuelle Router bestehen, unterscheidet der Parameter *Virtual Server ID* diese virtuelle Router voneinander. Beim Haupt- und beim Reserverouter muss dieser Parameter gleich eingestellt werden. Zum Hauptrouter wird der Router, der die mit dem Parameter *Host Priority* höhere Priorität eingestellt hat. In Abhängigkeit von RFC 2338 hat der Hauptrouter die



höchstmögliche Priorität, und zwar 255. Der Reserverrouter hat die Priorität im Grenzbereich 1 – 254 (Ausgangswert ist 100). Der Wert der Priorität gleich 0 ist nicht erlaubt.

Im zweiten Fensterteil kann die Kontrolle des Verbindungsaufbaus über PPP (GPRS) durch das Ankreuzen der Option *Check PPP connection* gewählt werden. Der aktive Hauptrouter (Haupt-/Reserverouter) sendet dann selbst die Ping Abfragen an die angeführte IP Adresse (*Ping IP Address*) in regelmäßigen Zeitintervallen (*Ping Interval*) mit eingestellter Wartezeit auf die Antwort (*Ping Timeout*). Die Kontrolle der PPP Verbindung ist zur Erkennung der Durchgängigkeit auf der Trasse vorgesehen, auf deren Grundlage die Übertragung der Routerfunktion vom Haupt- auf den Reserverouter, bzw. umgekehrt erfolgt. Die Trasse wird für undurchgängig gehalten, falls auf die festgesetzte Anzahl der Ping Abfragen *(Ping Probes)* keine Antwort zurückkommt. Als Ping Adresse muss die IP Adresse benutzt werden, bei der sicher ist, dass sie immer erreichbar bleibt und an die es möglich ist, die ICMP Abfragen (z. B. des DNS Server Netzbetreibers) zu senden. Zur Überwachung der Durchgängigkeit auf der Trasse ist es auch möglich, den Parameter *Enable traffic monitoring* zu nutzen. Ist dieser Parameter eingestellt, wird dann, falls ein anderes Paket als Ping auf die überwachte Trasse ausgesendet wird, inspiziert, ob irgendeine Antwort bis zum Ping Timeout zurückkommt. Ist dies nicht der Fall, wird die ursprüngliche ausgesendete Nachricht für eine Prüfnachricht (als ob Ping ausgesendet worden wäre, worauf keine Antwort zurückgekommen ist) gehalten und dann erfolgt eine beschleunigte Prüfung (mit einem Intervall zwischen der Aussendung, das durch den Parameter *Ping Timeout* gegebenen ist) mittels der Ping Nachrichten, wobei die erste ausgesendete Ping Nachricht schon als die zweite Prüfnachricht in Reihe gilt, die mit dem Parameter *Ping Probes* begrenzt wird..

VRRP Configuration

☐ Enable VRRP

Virtual Server IP Address		
Virtual Server ID		
Host Priority		

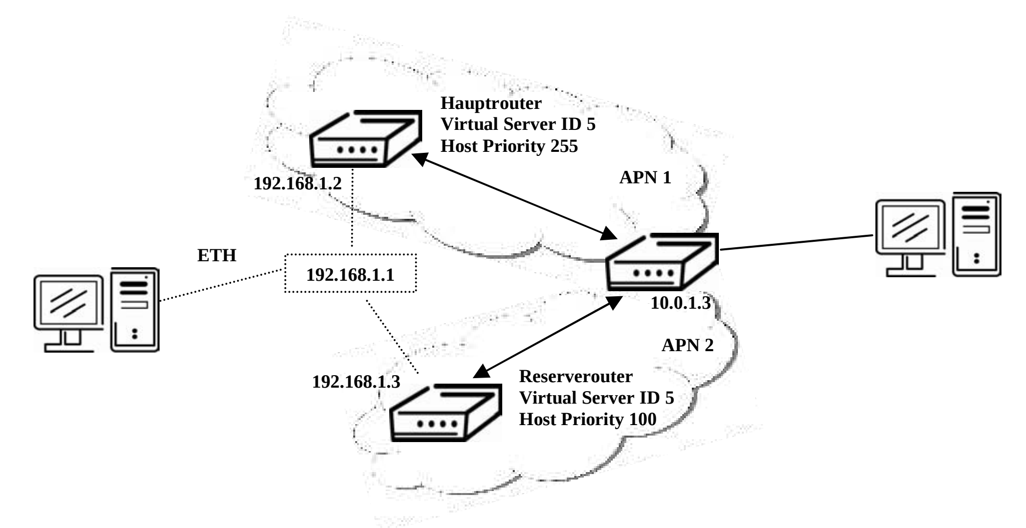
☐ Check PPP connection

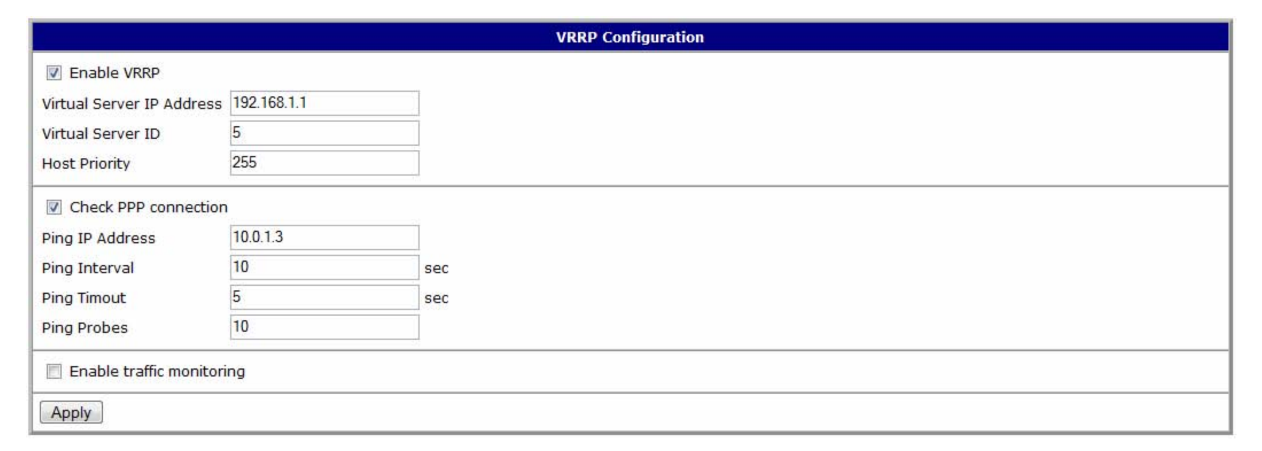
Ping IP Address		
Ping Interval		sec
Ping Timout		sec
Ping Probes		

☐ Enable traffic monitoring

Apply

Beispiel für die Einstellung des Protokolls VRRP:





VRRP Configuration

☑ Enable VRRP

Virtual Server IP Address	192.168.1.1	
Virtual Server ID	5	
Host Priority	255	

☑ Check PPP connection

Ping IP Address	10.0.1.3	
Ping Interval	10	sec
Ping Timout	5	sec
Ping Probes	10	

☐ Enable traffic monitoring

Apply

4.9. Konfiguration des Verbindungsaufbaus in GPRS

Die Konfiguration des Verbindungsaufbaus in GPRS kann durch die Auswahl der Option GPRS im Menü aufgerufen werden. Ist die Option *Create GPRS connection angekreuzt*, versucht der Router selbst nach dem Einschalten die GPRS Verbindung herzustellen. Im Fenster können *APN*, Benutzername (*Username*), Zutrittspasswort (*Password*) und die IP Adresse (*IP Address*) für zwei verschiedene APN definiert werden. Falls das Feld *IP Address* nicht ausgefüllt wird, wird die IP Adresse beim Verbindungsaufbau automatisch vom Netzbetreiber zugeteilt. Durch das Ausfüllen der vom Netzbetreiber zur Verfügung gestellten IP Adresse wird der Anschluss des Routers ans Netz beschleunigt.

Falls das Feld *APN* unausgefüllt bleibt, wählt der Router das APN automatisch laut dem IMSI Code der SIM Karte aus. Falls PLMN (Netzbetreibercode) nicht in der APN Liste ist, wird die Ausgangs-APN „Internet“ genutzt. APN wird vom Mobilnetzbetreiber definiert. Der Parameter PLMN kann in der Option *Operator* definiert werden. Mit dem Parameter *PIN* ist es möglich, den PIN Code in die SIM Karte bei jedem Starten des Routers einzugeben.



Vorsicht! Steckt nur eine SIM Karte im Router, die zwei verschiedene APN eingestellt hat, darf der Router keinen Halter für die zweite SIM Karte haben, ansonsten erfolgt nicht die richtige Umschaltung auf die zweite im Webformular definierte APN. Auch muss der richtige PIN Code angegeben werden, für die SIM Karte mit zwei APN ist der

PIN für beide APN gleich, ansonsten kann es zum Sperren der SIM Karte durch die mehrfache Eingabe des falschen PIN Codes kommen.

Die Auswahl der Option *Get DNS Address from Operator* ist für die einfachere Konfiguration auf Seiten des Kunden bestimmt. Ist diese Option angekreuzt, versucht der Router die IP Adressen des primären und sekundären DNS Servers vom Netzbetreiber automatisch zu ermitteln.

Ist die Option *Check PPP Connection* angekreuzt, wird die Kontrolle des Verbindungsaufbaus über PPP aktiviert. Der Router sendet dann selbst die Ping Abfragen an die angeführte IP Adresse (*Ping IP Address*) in regelmäßigen Zeitintervallen (*Ping Interval*). Gelingt es nicht, Ping an die angeführte IP Adresse 3x nacheinander zu senden, beendet der Router die bestehende Verbindung und versucht eine neue herzustellen. Die Kontrolle kann separat für zwei SIM Karten oder für zwei APN eingestellt werden. Als Ping Adresse kann die IP Adresse benutzt werden, bei der sicher ist, dass sie immer funktionsfähig bleibt und an die es möglich ist die ICMP Ping Abfragen (z. B. DNS Server des Netzbetreibers) zu senden.

Ist die Funktion *Enable Traffic Monitoring* angekreuzt, hört der Router auf, die Ping Abfragen an die *Ping IP Address* zu senden und überwacht den PPP Verbindungsaufbau. Beim Nullbetrieb in einem Zeitintervall, der länger als der *Ping Interval* ist, sendet der Router eine Abfrage an die Adresse *Ping IP Address.*

Der Parameter *Data Limit* stellt den Grenzwert der Datensendung über GPRS ein. Mit dem Parameter *Accounting Start* ist es möglich zu präzisieren, nach welcher Datenmenge die im Parameter *Data Limit* eingestellte Verrechnung gestartet wird. Ist der Parameter *Switch to Backup SIM Card When Data Limit Is Exceeded* (siehe unten) oder *Send SMS When Data Limit Is Exceeded* (siehe SMS Konfiguration) nicht angekreuzt, wird der Datengrenzwert nicht berechnet.

Der Parameter *Warning Threshold* gibt den prozentualen Wert des Parameters *Data Limit* an, nach dessen Überschreitung der Router eine SMS in der Form Router has exceeded (Wert des Parameters *Warning Threshold*) of Data Limit sendet.

Im unteren Teil der Konfiguration ist es möglich, die Regel zum Umschalten zwischen zwei APN auf einer SIM Karte, und zwar falls nur eine SIM Karte im Router (ER 75i oder ER 75i SL) eingelegt wird, oder zum Umschalten zwischen zwei SIM Karten, falls zwei SIM Karten in den Router (ER 75i DUO) eingelegt werden, einzustellen. Der Parameter *Default SIM card* stellt die Ausgangs-APN oder Ausgangs-SIM Karte ein, von der aus versucht wird die PPP Verbindung aufzubauen. Bei der Einstellung dieses Parameters auf *None* startet der Router im Offline Modus und die PPP Verbindung muss mittels einer SMS Nachricht aufgebaut werden. Beim Ausfall der PPP Verbindung stellt der freigegebene Parameter *Switch to Other SIM Card When Connection Fails* das Umschalten auf die zweite SIM Karte oder die zweite APN sicher. Falls das Roaming erfasst wird, ermöglicht der Parameter *Switch to Backup SIM Card When Roaming Is Detected* das Umschalten auf die zweite SIM Karte oder zweite APN. Der Parameter *Switch to Backup SIM Card When Data Limit Is Exceeded* stellt das Umschalten auf die zweite SIM Karte oder zweite APN im Falle der Überschreitung des Datengrenzwertes, der im Parameter *Data Limit* eingestellt wurde. Mit dem Parameter *Switch to Primary SIM Card after Timeout* ist es möglich, die Art zu definieren, auf welche der Router versucht zurück auf die Ausgangs-SIM Karte oder Ausgangs-APN umzuschalten.

Der Parameter *Initial Timeout* stellt die Zeit ein, nach deren Ablauf der Router versucht von der zweiten APN auf die Ausgangs-APN zurück zu schalten, der Bereich dieses Parameters beträgt 1 bis 10 000 Minuten. Der Parameter *Subsequent Timeout* stellt die Zeitperiode des Versuches ein, eine weitere Anmeldung zur Ausgangs-APN zu realisieren, der Bereich beträgt 1 bis 10 000 Minuten. Der Parameter *Additive Constant* gibt die Zeit ein, um welche die Zeit beim Versuch, die Hauptverbindung herzustellen, nach dem als erfolglosen

definierten Versuch verlängert wird (z. B. nach dem zweiten erfolglosen Versuch die Hauptverbindung aufzubauen, wird die Zeit des weiteren Versuchs um 30 Minuten verlängert usw.). Der Bereich beträgt 1 bis 1 000 Minuten.



Vorsicht! Wir empfehlen, falls der Router ununterbrochen läuft, die Funktion Check GPRS Connection zu verwenden.

Die Änderungen der Einstellung wirken sich nach der Betätigung der Taste *Apply* aus.

GPRS Configuration

☑ Create PPP connection

	Primary SIM card	Secondary SIM card	
APN *			
Username *			
Password *			
IP Address *			
Operator *			
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes

☑ Get DNS addresses from operator

☐ Check PPP connection (*necessary for uninterrupted operation*)

Ping IP Address			
Ping Interval			min

☐ Enable traffic monitoring

Data Limit		MB
Warning Threshold		%
Accounting Start	1	

Default SIM card	primary
Backup SIM card	secondary

☐ Switch to other SIM card when connection fails
☐ Switch to backup SIM card when roaming is detected
☐ Switch to backup SIM card when data limit is exceeded
☐ Switch to primary SIM card after timeout

Initial Timeout	60	min
Subsequent Timeout *		min
Additive Constant *		min

* *can be blank*

[Apply]

Anmerkung

- MTU (Maximum Transmission Unit) – identifiziert die maximale Paketgröße, für die das Element in der gegebenen Umgebung das Übertragungsvermögen hat. Vom Herstellerwerk ist die Größe auf 1 500 Bytes eingestellt.
- MRU (Maximum Receiving Unit) – identifiziert die maximale Paketgröße, für die das Element in der gegebenen Umgebung das Empfangsvermögen hat. Vom Herstellerwerk ist die Größe auf 1 500 Bytes eingestellt.

Bei der Einstellung einer fehlerhaften Größe kann es vorkommen, dass die Datenübertragung nicht korrekt verläuft.



4.10. Firewall Konfiguration

Mit der Firewall können die IP Adressen eingestellt werden, von denen der Fernzutritt zum Router möglich ist. Die Auswahl der Option *Allow Remote Access Only from Specified Hosts* schaltet die Firewall ein/aus. In der Firewall ist es möglich, bis zu acht Fernzutritte mittels der Parameter *Source*, *Source IP Address*, *Protocol* und *Target Port* einzustellen.

Der Parameter *Source* definiert, ob der Zutritt der einzigen IP Adresse, die als *Source IP Address* definiert wird, oder jeder beliebigen IP Adresse freigegeben wird. Im Menü *Protocol* ist es möglich zu präzisieren mit welchem Protokoll der Zutritt freigegeben wird, es kann der Zutritt für alle Protokolle (*all*) oder für die Protokolle *UDP*, *TCP* oder *ICMP* gewählt werden. Mit dem Parameter *Target Port* ist es möglich, die Anschlussnummer ausführlicher einzustellen.

Die Änderungen der Einstellung wirken sich nach der Betätigung der Apply Taste aus.



Vorsicht! Firewall filtriert nicht die Verbindung über Ethernet.

Firewall Configuration

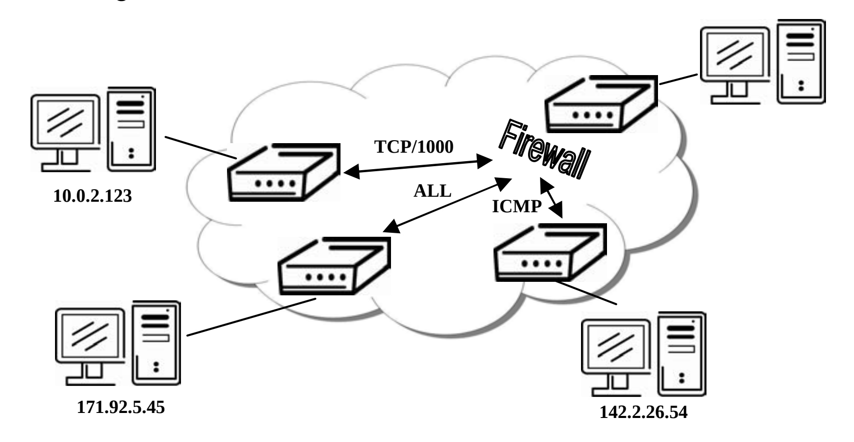
☐ Allow remote access only from specified hosts

Source	Source IP Address *	Protocol	Target Port *
single address		all	
single address		all	
single address		all	
single address		all	
single address		all	
single address		all	
single address		all	
single address		all	

* can be blank

Apply

Beispiel für die Einstellung der Firewall



Firewall Configuration

☑ Allow remote access only from specified hosts

Source	Source IP Address *	Protocol	Target Port *
single address	171.92.5.45	all	
single address	10.0.2.123	TCP	1000
single address	142.2.26.54	ICMP	
single address		all	
single address		all	
single address		all	
single address		all	
single address		all	

* can be blank

Apply

4.11. Konfiguration der Adressenübersetzung (NAT)

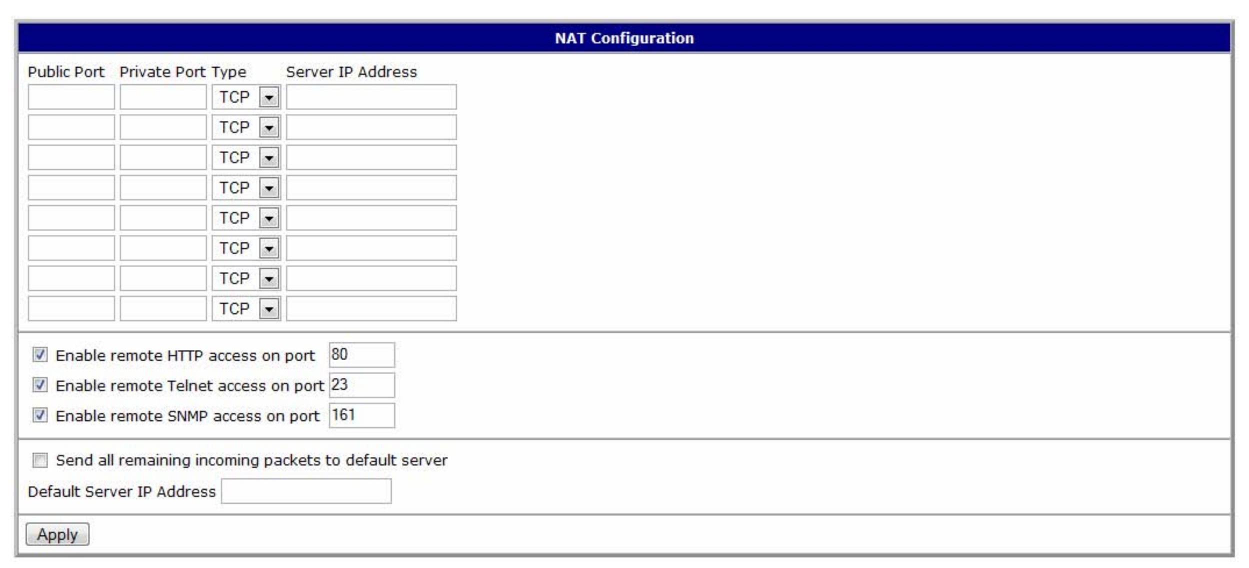
Die Konfiguration der Adressenübersetzung kann durch die Auswahl der Option NAT im Menü aufgerufen werden. Das Fenster beinhaltet acht Optionen zur Bestimmung der Adressenübersetzung, jede Zeile enthält den Außenanschluss, Innenanschluss, die Auswahl des Protokolls TCP/UDP und die IP Adresse, an die die ankommenden Daten gesandt werden. Durch das Ankreuzen der Option *Send All Incoming Packets to Default Server* und durch die Einstellung der Option *Default Server* kann der Router in einen Modus gebracht werden, in dem er die sämtliche ankommende Kommunikation von GPRS an einen Computer mit definierter IP Adresse weiterleitet.

Durch das Ankreuzen der Option *Enable Remote http Access on Port* und durch die Eingabe der Anschlussnummer ist es möglich, die Konfiguration des Routers über eine Webschnittstelle vorzunehmen.

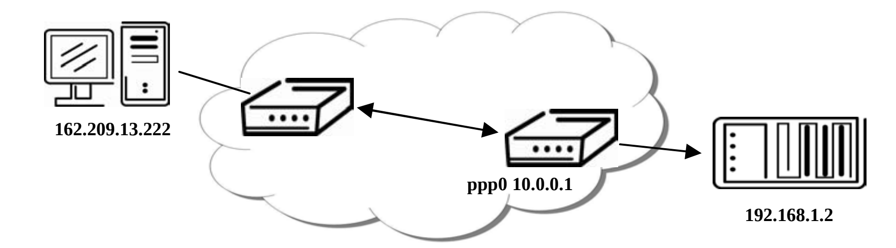
Die Auswahl der Option *Enable RemoteTelnet Access on Port* und die Eingabe der Anschlussnummer ermöglichen den Zutritt über *Telnet*.

Die Auswahl der Option *Enable Remote SNMP Access on Port* und Eingabe der Anschlussnummer bietet die Möglichkeit der Abfragen des SNMP Agenten frei.

Die Änderungen der Einstellung wirken sich nach der Betätigung der Taste *Apply* aus.



Beispiel für die Konfiguration mit einem an den Router angeschlossenen Gerät:



NAT Configuration

Public Port	Private Port	Type	Server IP Address
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

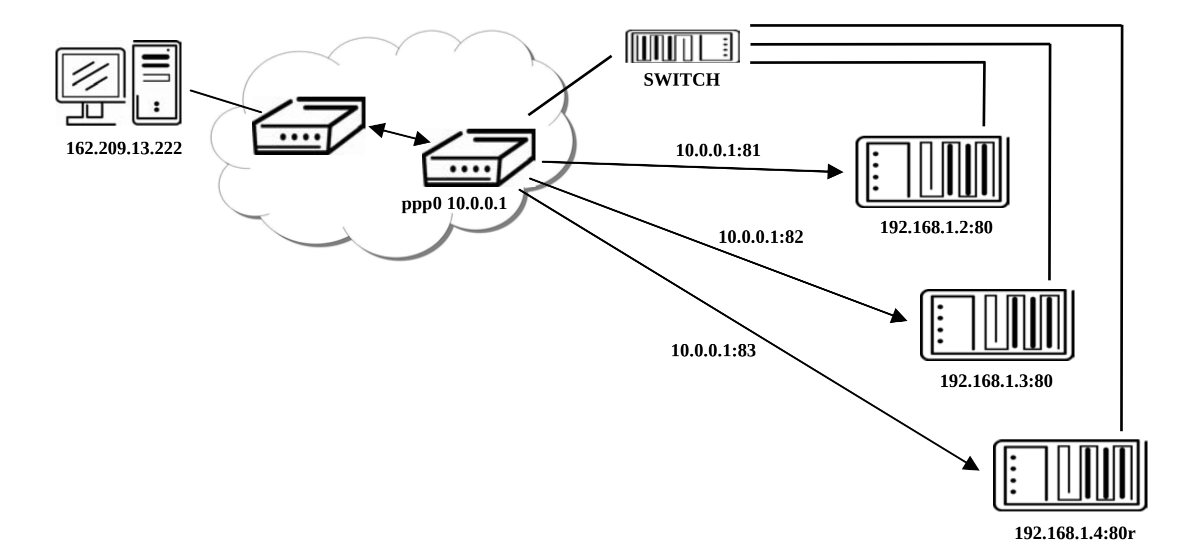
☑ Enable remote HTTP access on port 80
☑ Enable remote Telnet access on port 23
☑ Enable remote SNMP access on port 161

☑ Send all remaining incoming packets to default server
Default Server IP Address 192.168.1.2

Apply

Bei dieser Konfiguration ist es wichtig, die Option *Send All Remaining Incoming Packets to Default Server* gekennzeichnet zu haben, die IP Adresse ist in diesem Falle die Adresse des hinter den Router angeschlossenen Gerätes. Das hinter den Router angeschlossene Gerät muss das Ausgangsgateway auf den Router eingestellt haben. Bei PING an die IP Adresse der SIM Karte antwortet das angeschlossene Gerät.

Beispiel für die Konfiguration mit mehreren Geräten am Router:



NAT Configuration

Public Port	Private Port	Type	Server IP Address
81	80	TCP	192.168.1.2
82	80	TCP	192.168.1.3
83	80	TCP	192.168.1.4
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

☑ Enable remote HTTP access on port 80
☑ Enable remote Telnet access on port 23
☑ Enable remote SNMP access on port 161

☐ Send all remaining incoming packets to default server
Default Server IP Address

Apply

Bei dieser Konfiguration definieren die Adressen *Server IP Address* das hinter den Router angeschlossene Gerät. Bei Ping an die IP Adresse der SIM Karte antwortet der Router. Der Zutritt auf die Webschnittstelle des hinter den Router angeschlossenen Gerätes ist mit Port Forwarding möglich, bei dem der Außenanschluss, zu dem der Zutritt erwünscht wird, hinter die IP Adresse SIM angeführt wird. Beim Bedarf für den Anschluss 80 werden die einzelnen Außenanschlüsse (Public Port) geprüft, dort ist dieser Anschluss nicht definiert, darum wird bei der angekreuzten Option *Enable Remote HTTP Access* die Webschnittstelle des Routers automatisch geöffnet. Ist diese Option nicht angekreuzt und ist die Option *Send All Remaining Incoming Packets to Default Server* auc nicht angekreuzt, wird die Verbindung an die angeführte IP Adresse verwirklicht. Sind die Option der Webschnittstelle und die *Default Server IP Address* nicht angekreuzt, wird die Anforderung nicht durchgeführt.

Falls es erforderlich ist, mehr als 8 Regeln für NAT einzustellen, ist es möglich, folgendes Skript im Start-Up Script Window einzufügen:

iptables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT --to-destination [IPADDR]:[PORT1_PRIVATE],

wo die sachlichen Anschlussnummern anstatt von [PORT_PUBLIC] und [PORT1_PRIVATE] einzufügen sind und die IP Adresse anstatt von [IPADDR] einzufügen ist.

4.12. Konfiguration des OpenVPN Tunnels

Die Konfiguration des OpenVPN Tunnels kann durch die Auswahl der Option OpenVPN im Menü aufgerufen werden. Der OpenVPN Tunnel ermöglicht eine sichere (verschlüsselte) Verbindung von zwei LAN Netzen in ein Netz, das sich als homogen anstellt. Der OpenVPN Tunnel wird nach dem Ankreuzen der Option *Create OpenVPN Tunnel* aufgebaut.

Im Fenster kann das Protokoll (*Protocol*) definiert werden, mithilfe dessen OpenVPN die Kommunikation führt. Zur Auswahl steht das Protokoll *UDP*, *TCP Server* oder *TCP Client*, zu denen der Anschluss des Protokolls zugeteilt werden muss. Die Parameter definieren: *Remote IP Address* die IP Adresse der gegenüberliegenden Tunnelseite, *Remote Subnet* die Adresse vom Netz hinter der gegenüberliegenden Tunnelseite und *Remote Subnet Mask* die Maske vom Netz hinter der gegenüberliegenden Tunnelseite. Der Parameter *Redirect Gateway* ermöglicht den gesamten Verkehr im Ethernet umzulenken. Der Parameter *Local Interface IP Address* definiert die IP Adresse der lokalen Schnittstelle und der Parameter *Remote Interface IP Address* definiert die IP Adresse der Schnittstelle auf der gegenüberliegenden Tunnelseite. Der Parameter *Ping Interval* definiert das Zeitintervall, nach dessen Ablauf die Nachricht der gegenüberliegenden Seite gesendet wird und durch die Einstellung des Parameters *Ping Timeout* wird eine von der gegenüberliegenden Seite gesandte Nachricht abgewartet. Zur richtigen Verifizierung des OpenVPN Tunnels muss der Parameter *Ping Timeout* größer als *Ping Interval* sein. Der Parameter *Renegotiate Interval* stellt die Periode der erneuten Negotiation (der erneuten Autorisierung) des OpenVPN Tunnels ein. Dieser Parameter kann nur bei der Verifizierung des User Names/Passwords oder bei Verwendung des Zertifikats X.509 eingestellt werden. Mit dem Parameter *Max Fragment Size* ist es möglich, die maximale Größe des abgesandten Pakets zu definieren. Die abgesandten Daten können mit verlustfreier LZO Komprimierung im Parameter *Compression* verdichtet werden, die Komprimierung muss an beiden Tunnelseiten eingestellt werden. Im Parameter *NAT Rules* können die eingestellten NAT Regeln auf den OpenVPN Tunnel angewandt werden oder diese Anwendung muss nicht erfolgen. Mit dem Parameter *Authenticate Mode* ist es möglich, die Authentisierung einzustellen. Zur Auswahl stehen auch: keine Authentisierung (None), oder Authentisierung mittels *Pre-shared Secret*, mit diesem Parameter wird ein geteilter Schlüssel für beide Tunnelseiten eingestellt; oder *User Name / Password,* dieser Parameter ermöglicht die Authentisierung mittels *CA Certificate*, *User Name* und *Password*; oder *X.509 Certificate (Client),* der Parameter ermöglicht die Authentisierung mittels *CA Certificate*, *Local Certificate* und *Local Private Key*; oder aber *X.509 Certificate (Server)*, der Parameter ermöglicht die Authentisierung mittels *CA Certificate*, *DH Parameters*, *Local Certificate* und *Local Private Key*.

OpenVPN Tunnel Configuration

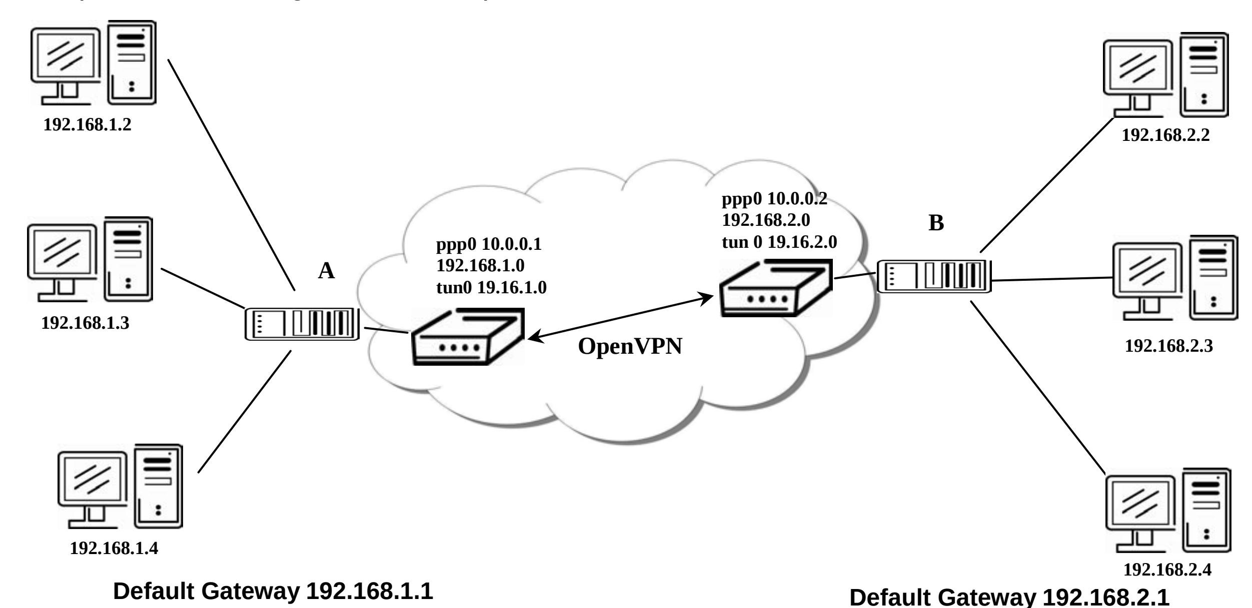
☐ Create OpenVPN tunnel

Protocol	UDP	
UDP port	1194	
Remote IP Address *		
Remote Subnet *		
Remote Subnet Mask *		
Redirect Gateway	no	
Local Interface IP Address		
Remote Interface IP Address		
Ping Interval *		sec
Ping Timeout *		sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	none	
Pre-shared Secret		
CA Certificate		
DH Parameters		
Local Certificate		
Local Private Key		
Username		
Password		

** can be blank*

Apply

Beispiel für die Konfiguration des OpenVPN Tunnels:



Konfiguration des OpenVPN Tunnels:

	A	B
Protocol	UDP	UDP
UDP Port 1194	1194	
Remote IP Address:	10.0.0.2	10.0.0.1
Remote Subnet:	192.168.2.0	192.168.1.0
Remote Subnet Mask:	255.255.255.0	255.255.255.0
Local Interface IP Address:	19.16.1.0	19.16.2.0
Remote Interface IP Address:	19.16.2.0	19.18.1.0
Compression	LZO	LZO
Authenticate mode:	none	none

4.13. Konfiguration des IPSec Tunnels

Der IPsec Tunnel erzeugt eine sichere (verschlüsselte) Verbindung von zwei LAN Netzen in ein Netz, das sich als homogen anstellt. Der Router bietet die Möglichkeit bis zu vier IPsec Tunnel zu erzeugen, deren Konfiguration durch die Auswahl der Option *IPsec* im Menü aufgerufen werden kann. Im Fenster *IPsec Tunnels Configuration* sind vier Zeilen, jede Zeile entspricht der Konfiguration von jeweils einem Tunnel. Die Spalte *Create* schaltet die einzelnen Tunnel ein, die anderen Spalten beinhalten die Ansicht der im Fenster *IPsec Tunnel Configuration* eingestellten Werte, dieses Fenster wird durch die Betätigung der Taste *Edit* angezeigt.

IPsec Tunnels Configuration

	Create	Description	Remote IP Address	Remote Subnet	
1st	no				Edit
2nd	no				Edit
3rd	no				Edit
4th	no				Edit

Apply

Im Fenster *IPsec Tunnel Configuration* können die Tunnelbezeichnung (*Description*), die IP Adresse der gegenüberliegenden Tunnelseite (*Remote IP Address*), die ID der gegenüberliegenden Seite (*Remote ID*), die Adresse vom Netz hinter der gegenüberliegenden Tunnelseite (*Remote Subnet*), die Maske vom Netz hinter der gegenüberliegenden Tunnelseite (*Remote Subnet Mask*), die ID der lokalen Seite (*Local ID*), die Adresse vom Lokalnetz (*Local Subnet*), die Maske vom Lokalnetz (*Local Subnet Mask*), die Lebensdauer vom Schlüssel (*Key Lifetime*) und die Lebensdauer von IKA SA (*IKE lifetime*) definiert werden. Der Parameter *Rekey Margin* bestimmt die Zeit vor dem Ablauf der Gültigkeit der Schlüssel, wenn neue Schlüssel erzeugt werden. Darüber hinaus wird diese Zeit bis um *Rekey Fuzz* Prozente vom Wert des Parameters Rekey Margin zufälligerweise verlängert. Wird die Adressenübersetzung zwischen zwei Endpunkten des IPsec Tunnels benutzt, ist es notwendig NAT Traversal (*Enabled*) freizugeben. Durch das Ankreuzen des Parameters *Aggressive Mode* wird der angreifende Modus beim Verbindungsaufbau eingestellt. Die Verbindung wird dann schneller aufgebaut, aber die Verschlüsselung wird auf 3DES-MD5 fest eingestellt. Die Authentisierung kann mit dem Parameter *Authenticate mode* eingestellt werden, zur Auswahl stehen die Möglichkeiten *Pre-shared Key* oder Zertifikat *X.509*. MIt dem Parameter *Pre-shared Key* wird dann der geteilte Schlüssel für beide Tunnelseiten eingestellt. Bei der Authentisierung mit dem Zertifikat X.509 sind die Zertifikate *CA Certificate*, *Remote Certificate, Local Certificate*, Privatschlüssel *Local Private Key* und *Local Passphrase* einzufügen. Die Zertifikate und der Privatschlüssel müssen im Format PEM sein. Als Zertifikat kann nur ein solches Zertifikat benutzt werden, das mit Anfang und Ende des Zertifikats eingeleitet wird. Die Parameter ID setzen sich aus zwei Teilen, H*ost Name* und D*omain Name,* zusammen. Die Optionen, die leer sein können, werden zur genauen Identifizierung vom IPsec Tunnel benutzt.

Die Änderungen der Einstellung wirken sich nach der Betätigung der Apply Taste aus.

IPsec Tunnel Configuration

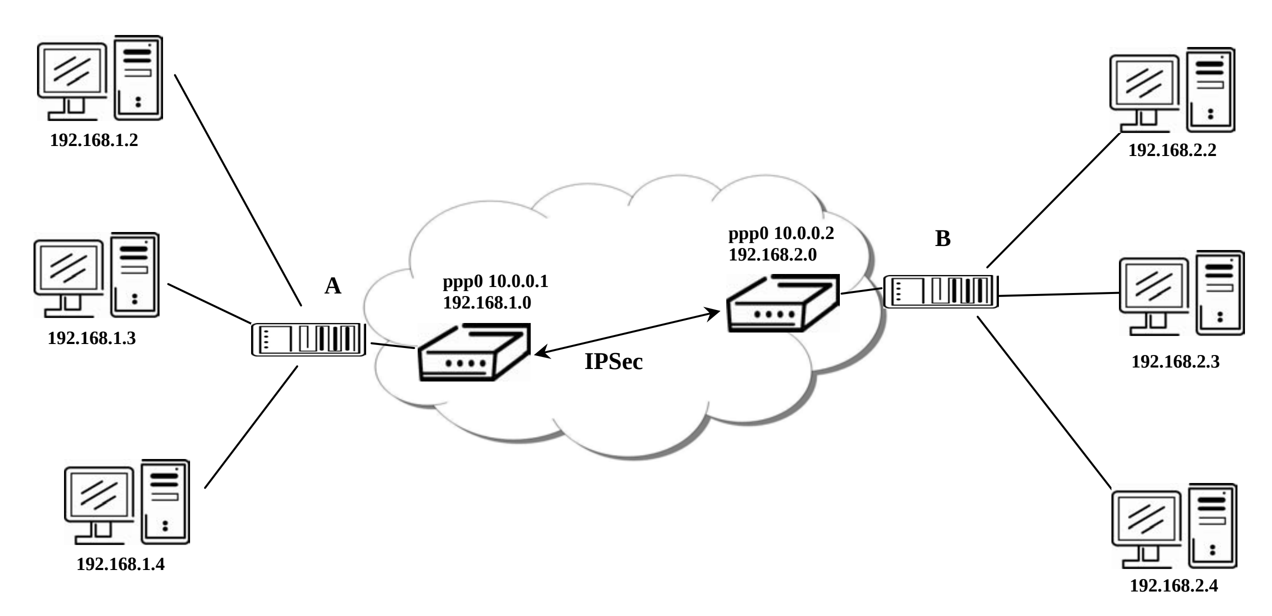
☐ Create 1st IPsec tunnel

Description *		
Remote IP Address *		
Remote ID *		
Remote Subnet *		
Remote Subnet Mask *		
Local ID *		
Local Subnet *		
Local Subnet Mask *		
Key Lifetime	3600	sec
IKE Lifetime	3600	sec
Rekey Margin	540	sec
Rekey Fuzz	100	%
NAT Traversal	disabled	
Aggressive Mode	disabled	
Authenticate Mode	pre-shared key	
Pre-shared Key		
CA Certificate		
Remote Certificate		
Local Certificate		
Local Private Key		
Local Passphrase *		

** can be blank*

Apply

Beispiel für die Konfiguration des IPSec Tunnels:



Default Gateway 192.168.1.1 **Default Gateway 192.168.2.1**

Konfiguration des IPSec Tunnels:

	A	B
Remote IP Address:	10.0.0.2	10.0.0.1
Remote Subnet:	192.168.2.0	192.168.1.0
Remote Subnet Mask:	255.255.255.0	255.255.255.0
Local Subnet:	192.168.1.0	192.168.2.0
Local Subnet Mask:	255.255.255.0	255.255.255.0
Authenticate mode:	pre-shared key	pre-shared key
Pre-shared key	test	test

4.14. Konfiguration des GRE Tunnels

Der GRE Tunnel erzeugt eine Verbindung von zwei LAN Netzen in ein Netz, das sich als homogen anstellt. Der Router bietet die Möglichkeit, bis zu vier GRE Tunnel zu erzeugen, deren Konfiguration durch die Auswahl der Option *GRE* im Menü aufgerufen werden kann. Im Fenster *GRE Tunnels Configuration* sind vier Zeilen, jede Zeile entspricht der Konfiguration von jeweils einem Tunnel. Die Spalte Create schaltet die einzelnen Tunnel ein, die anderen Spalten beinhalten die Ansicht der im Fenster *GRE Tunnel Configuration* eingestellten Werte, dieses Fenster wird durch Betätigung der Taste *Edit angezeigt.*

GRE Tunnels Configuration

	Create	Description	Remote IP Address	Remote Subnet	
1st	no				Edit
2nd	no				Edit
3rd	no				Edit
4th	no				Edit

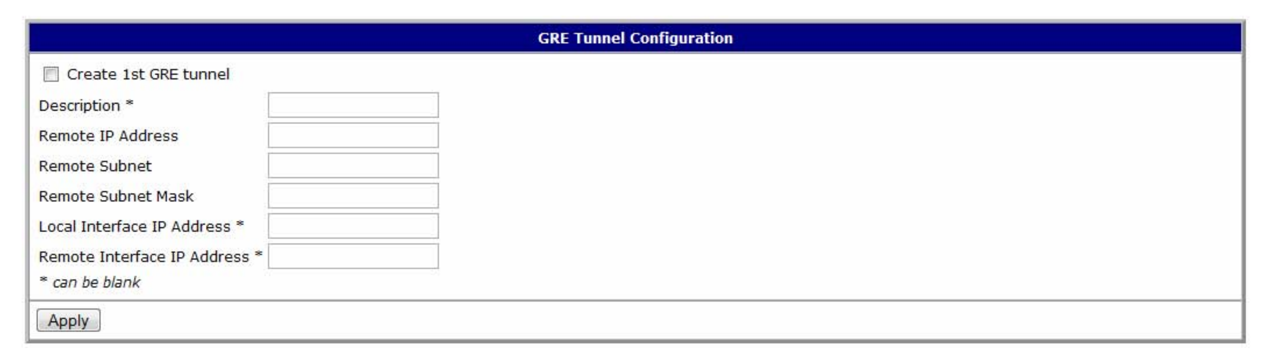
Apply

Die Tunnel werden durch das Ankreuzen der Option *Create x GRE Tunnel* aktiviert. Weiter können die Bezeichnung des GRE Tunnels (*Description*), die IP Adresse der gegenüberliegenden Tunnelseite (*Remote IP Address*), die interne IP Adresse des Tunnels auf der lokalen Tunnelseite (*Local Interface IP Address*), die interne IP Adresse der gegenüberliegenden Tunnelseite (*Remote Interface IP Address*), die Adresse vom Netz hinter der gegenüberliegenden Tunnelseite (*Remote Subnet*) und die Maske vom Netz hinter der gegenüberliegenden Tunnelseite (*Remote Subnet Mask*) definiert werden.

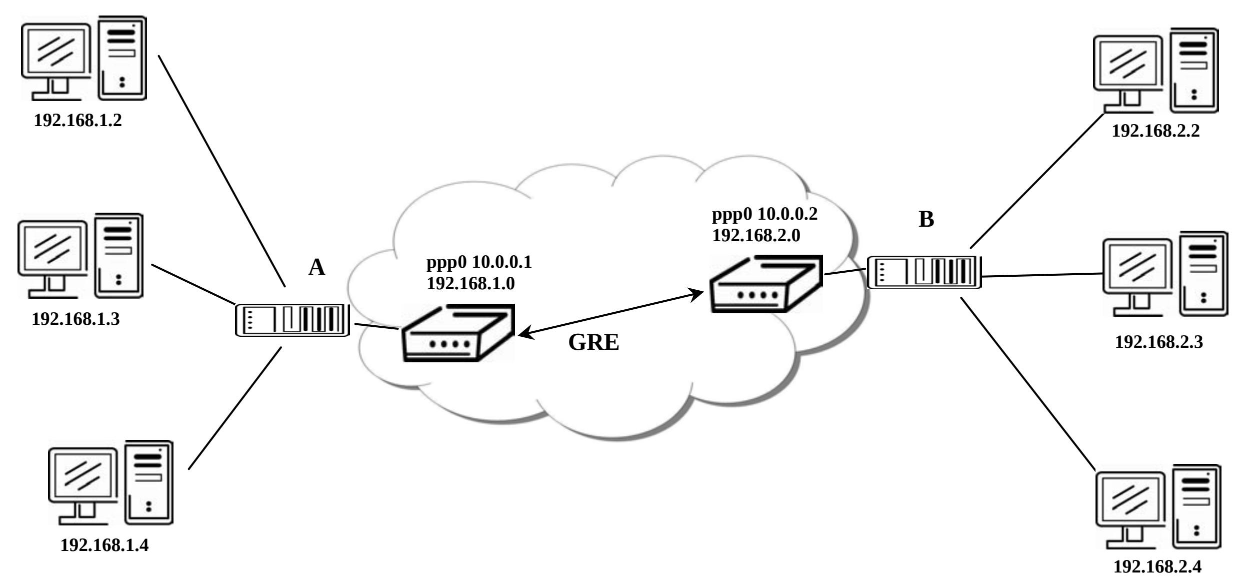


Vorsicht, der GRE Tunnel kommt an der Übersetzung der NAT Adressen nicht weiter.

Die Änderungen der Einstellung wirken sich nach der Betätigung der Apply Taste aus.



Beispiel für die Konfiguration des GRE Tunnels:



Konfiguration des GRE Tunnels:

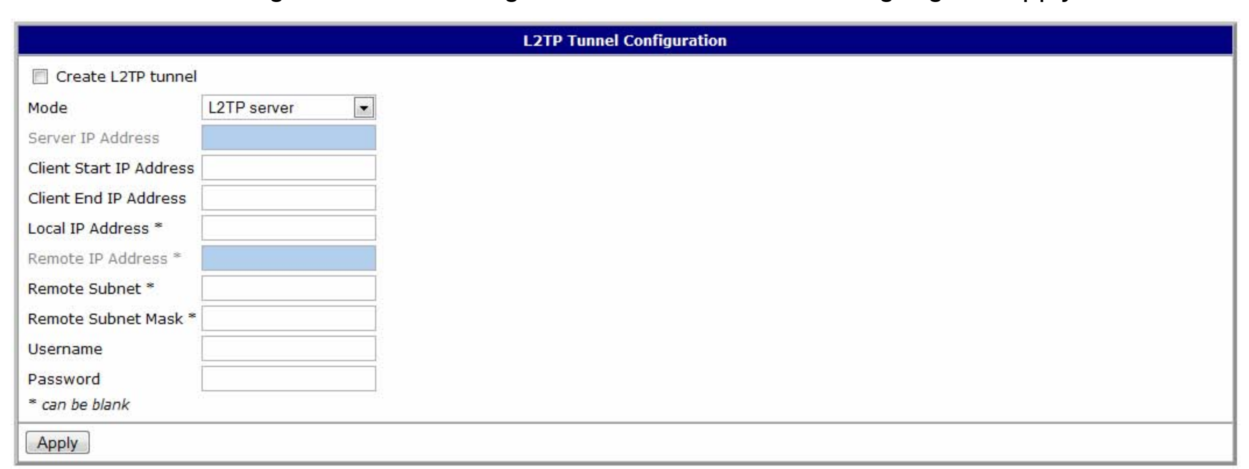
	A	B
Remote IP Address:	10.0.0.2	10.0.0.1
Remote Subnet:	192.168.2.0	192.168.1.0
Remote Subnet Mask:	255.255.255.0	255.255.255.0

4.15. Konfiguration des L2TP Tunnels

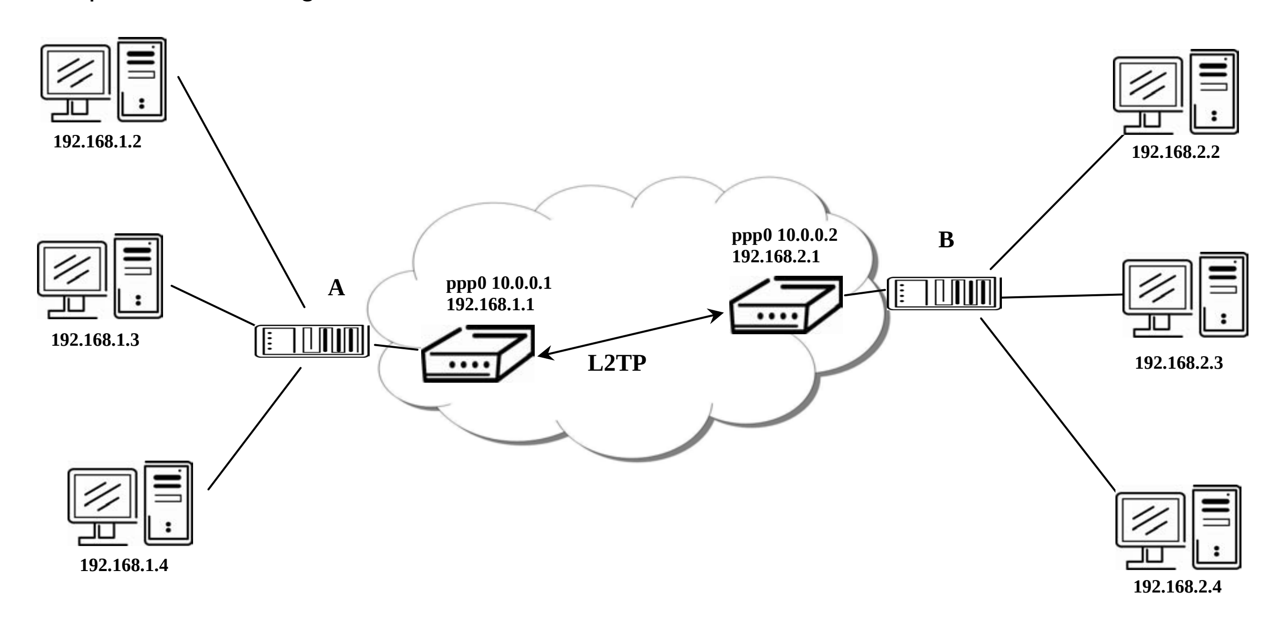
Die Konfiguration des L2TP Tunnels kann durch die Auswahl der Option L2TP im Menü aufgerufen werden. Der L2TP Tunnel wird zur Verbindung von zwei LAN Netzen in ein Netz mit Authentisierung benutzt, wobei sich das Netz als homogen anstellt. Der L2TP Tunnel wird nach dem Ankreuzen der Option *Create L2TP Tunnel* aufgebaut.

Im Fenster können der Modus (*Mode*) des L2TP Tunnels auf der Routerseite, die IP Serveradresse (*Server IP Address*) bei Kunden, die vom Server den Klienten angebotene IP Anfangsadresse (*Client Start IP Address*), die vom Server den Klienten angebotene IP Endadresse (*Client End IP Address*), die IP Adresse des Tunnels auf der lokalen Seite (*Local IP Address*), die IP Adresse der gegenüberliegenden Tunnelseite (*Remote IP Address*), die Adresse vom Netz hinter der gegenüberliegenden Tunnelseite (*Remote Subnet*), die Maske vom Netz hinter der gegenüberliegenden Tunnelseite (*Remote Subnet Mask*), der Anmeldungsname zur Anmeldung in den L2TP Tunnel (*User Name*) und das Passwort (*Password*) definiert werden.

Die Änderungen der Einstellung wirken sich nach der Betätigung der Apply Taste aus.



Beispiel für die Konfiguration des L2TP Tunnels:



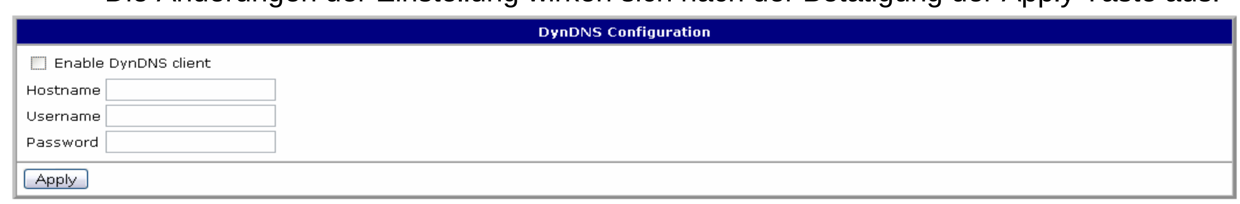
Konfiguration des L2TP Tunnels:

	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	---	10.0.0.1
Client Start IP Address:	192.168.1.2	---
Client End IP Address:	192.168.1.254	---
Local IP Address:	192.168.1.1	---
Remote IP Address	---	---
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	Benutzer	Benutzer
Password	Passwort	Passwort

4.16. Konfiguration des DynDNS Klienten

Die Konfiguration des DynDNS Klienten kann durch die Auswahl der Option DynDNS im Menü aufgerufen werden. Im Fenster können die am Server www.dyndns.org registrierte Domäne der dritten Größenordnung (*Hostname*), der Anmeldungsname (*User Name*) und Passwort (*Password*) definiert werden.

Die Änderungen der Einstellung wirken sich nach der Betätigung der Apply Taste aus.





Beispiel für die Konfiguration des DynDNS Klienten mit der Domäne conel.dyndns.org, dem Benutzernamen conel und Passwort conel:

DynDNS Configuration

Enable DynDNS client
Hostname conel.dyndns.org
Username conel
Password conel
Apply

Teilt der Netzbetreiber die DNS Server nicht zu, ist es möglich#, die Server durch das Einfügen vom Skript in Start-Up Script Window zu konfigurieren:

echo “nameserver xxx.xxx.xxx.xxx“ > /etc/resolf.conf, wo xxx.xxx.xxx.xxx ist die IP Adresse des ersten DNS Servers,

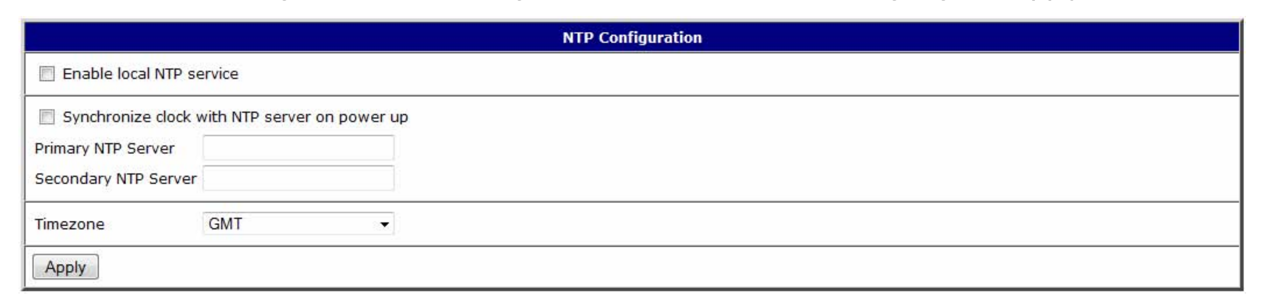
echo “nameserver yyy.yyy.yyy.yyy“ >> /etc/resolf.conf, wo yyy.yyy.yyy.yyy ist die IP Adresse des zweiten DNS Servers.

4.17. Konfiguration des NTP Klienten

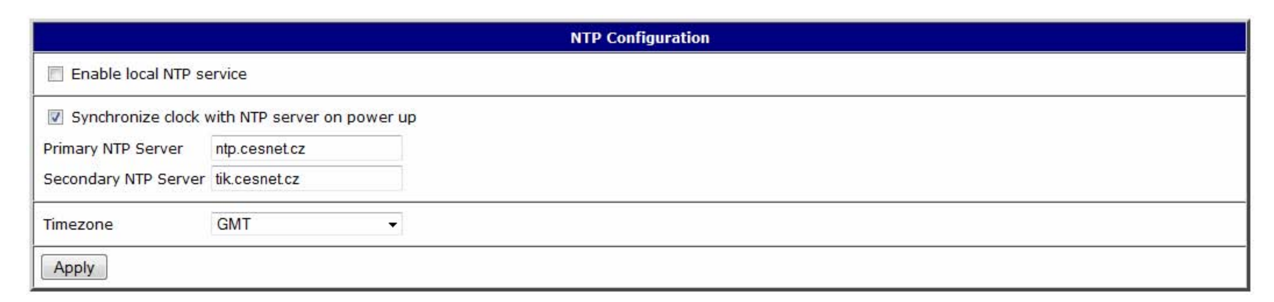
Die Konfiguration des NTP Klienten kann durch die Auswahl der Option NTP im Menü aufgerufen werden. Im Fenster können die Adressen des primären (*Primary NTP Server Address*) und des sekundären NTP Servers (*Secondary NTP Server Address*) definiert werden, mittels der der Router nach dem ersten Verbindungsaufbau in GPRS ab der Einschaltung der Stromversorgung die interne Uhr stellt. Beispiel für die Adresse des NTP Servers kann ntp.cesnet.cz und tik.cesnet.cz sein. Mit dem Parameter *Timezone* kann die Zeitzone des Routers eingestellt werden.

Der Parameter *Enable Local NTP Service* stellt den Router in den Modus, bei dem er als NTP Server für andere Geräte funktioniert.

Die Änderungen der Einstellung wirken sich nach der Betätigung der Apply Taste aus.



Beispiel für die Konfiguration von NTP mit dem eingestellten primären und sekundären NTP Server.



4.18. *Konfiguration des SNMP Agenten*

Durch das Aufrufen der Option SNMP ist die Konfiguration des SNMP Agenten Ver.1 möglich, der die Informationen über den Router bzw. über den Zustand des Erweiterungsanschlusses CNT oder MBUS sendet.

Die Option *Community* definiert das Passwort zum Zutritt zum SNMP Agenten. Die Option *Contact* identifiziert die Person, die den Router verwaltet, zusammen mit den Informationen, wie der Kontakt mit dieser Person aufzunehmen ist. Die Option *Name* ist die Benennung des Routers und die Option *Location* beschreibt die tatsächliche Unterbringung des Routers.

Durch das Ankreuzen der Option *Enable XC-CNT extension* ist es möglich, den Zustand der Eingänge am Erweiterungsanschluss CNT zu überwachen, oder durch Ankreuzen der Option *Enable M-BUS extension* und durch Einstellung der Geschwindigkeit der Kommunikation (*Baudrate*), der Parität (*Parity*) und der Anzahl von Stoppbits (*Stop Bits*) ist es möglich, den Zustand der angeschlossenen Messgeräte am Erweiterungsanschluss MBUS zu überwachen. Diese zwei Parameter können nicht gleichzeitig angekreuzt werden.

SNMP Configuration

- [x] Enable SNMP agent

Community: public
Contact *
Name *
Location *

- [ ] Enable XC-CNT extenstion

- [ ] Enable M-BUS extenstion

Baudrate: 300
Parity: even
Stop Bits: 1
* can be blank

Apply

Jeder überwachte Wert ist mittels des numerischen Identifikators **OID** – *Object Identifier* eindeutig identifiziert. OID endet mit „9”.

Für den Erweiterungsanschluss CNT wird der folgende OID Bereich (der internen Variablen) verwendet:

OID	Bedeutung
.1.3.6.1.4.1.30140.2.1.1.0	Analogeingang AN1 (Bereich 0-4095)
.1.3.6.1.4.1.30140.2.1.2.0	Analogeingang AN2 (Bereich 0-4095)
.1.3.6.1.4.1.30140.2.1.3.0	Zählereingang CNT1 (Bereich 0-4294967295)
.1.3.6.1.4.1.30140.2.1.4.0	Zählereingang CNT2 (Bereich 0-4294967295)
.1.3.6.1.4.1.30140.2.1.5.0	Binäreingang BIN1 (Werte 0,1)
.1.3.6.1.4.1.30140.2.1.6.0	Binäreingang BIN2 (Werte 0,1)
.1.3.6.1.4.1.30140.2.1.7.0	Binäreingang BIN3 (Werte 0,1)
..1.3.6.1.4.1.30140.2.1.8.0	Binäreingang BIN4 (Werte 0,1)

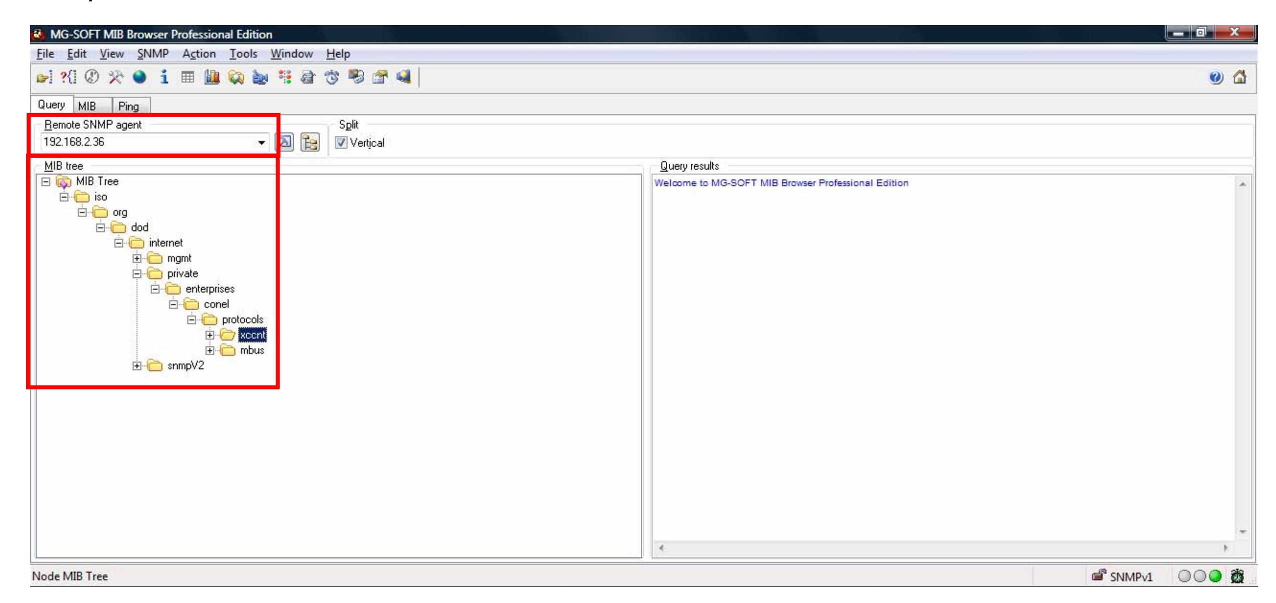
Für den Erweiterungsanschluss MBUS wird der folgende OID Bereich (der internen Variablen) verwendet:

OID	Bedeutung
.1.3.6.1.4.1.30140.2.2.<Adresse>.1.0	IdNumber – Nummer des Messgeräts
.1.3.6.1.4.1.30140.2.2.<Adresse>.2.0	Manufacturer – Hersteller
.1.3.6.1.4.1.30140.2.2.<Adresse>.3.0	Version – spezifiziert die Version des Messgeräts

.1.3.6.1.4.1.30140.2.2.<Adresse>.4.0	Medium – Typ des gemessenen Mediums
.1.3.6.1.4.1.30140.2.2.<Adresse>.5.0	Status – Meldungen der Fehlerzustände
.1.3.6.1.4.1.30140.2.2.<Adresse>.6.0	0. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<Adresse>.7.0	0. gemessener Wert
.1.3.6.1.4.1.30140.2.2.<Adresse>.8.0	1. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<Adresse>.9.0	1. gemessener Wert
...	
.1.3.6.1.4.1.30140.2.2.<Adresse>.100.0	47. VIF – Informationsfeld mit Wert
.1.3.6.1.4.1.30140.2.2.<Adresse>.101.0	47. gemessener Wert

Die Adresse des Messgerätes kann aus dem Bereich 0 bis 254 sein, wobei 254 Broadcast ist.

Beispiel für einen MIB Browser:



Es ist wichtig die IP Adresse vom SNMP Agenten (Router) im Feld *Remote SNMP agent* einzustellen. Nach der Eingabe der IP Adresse ist es im Teil *MIB tree* möglich die internen Variablen anzuzeigen. Der Pfad zu den Variablen ist:

iso->org->dod->internet->private->enterprises->conel->protocols

4.19. Konfiguration und SMS Versenden

Die SMS Konfiguration wird durch die Auswahl der Option *SMS* im Hauptmenü aufgerufen. Im ersten Fensterteil wird das Versenden der SMS konfiguriert. In der Konfiguration des SMS Versandes ist es möglich, das automatische Versenden einer SMS nach dem Einschalten der Stromversorgung (*Send SMS on Power Up*), beim Verbindungsaufbau (*Send SMS on PPP Connect*) oder beim Verlust der PPP Verbindung (*Send SMS on PPP Disconnect*) sowie bei Überschreitung des Datengrenzwerts (*Send SMS When Data Limit Exceeded*) einzustellen. Der Parameter *Send SMS When Binary Input Is Active* stellt das Versenden der SMS beim aktiven Binärausgang sicher, wobei der Text der SMS-Nachricht mit den Parametern BIN1-SMS bis BIN4-SMS festgelegt wird. Die Information wird bis auf drei Telefonnummern versendet. Das Feld *Unit ID* ist die Benennung des Routers, die gegebenenfalls in der SMS abgesandt wird, diese Benennung kann ein beliebiges Format haben.





Im zweiten Teil ist es möglich, die Betätigung des Routers mittels SMS Nachrichten zu konfigurieren. Nach dem Ankreuzen der Option *Enable remote control via SMS* ist es möglich, die *PPP* Verbindung mittels einer SMS Nachricht aufzubauen oder abzuschließen. Diese Betätigung kann für bis zu drei Telefonnummern eingestellt werden. Ist die Betätigung des Routers mittels SMS Nachrichten eingestellt, werden alle ankommenden SMS automatisch bearbeitet und gelöscht. In der Ausgangseinstellung ist dieser Parameter eingeschaltet.



Ist keine Telefonnummer ausgefüllt, ist es möglich den Router erneut zu starten, und zwar durch das Versenden der SMS Nachricht im Format *Reboot* von einer beliebigen Nummer aus. Sind eine oder mehrere Nummern ausgefüllt, ist es möglich, den Router mittels der nur von diesen Nummern gesandten SMS Nachrichten zu betätigen.

Es sind SMS im Format möglich:

SMS	Bedeutung
go online sim 1	Umschalten auf erste SIM (APN1)
go online sim 2	Umschalten auf zweite SIM (APN2)
go online	Der Router wird in den Modus Online umgeschaltet
go offline	Beendigung der PPP Verbindung
set out=0	Der Ausgang vom Anschluss CNT wird auf 0 gesetzt
set out=1	Der Ausgang vom Anschluss CNT wird auf 1 gesetzt
reboot	Neustart des Routers

Durch die Auswahl der Option *Enable AT-SMS Protocol on External Port* und durch die Einstellung der Geschwindigkeit (*Baudrate*) ist es möglich, das Versenden / den Empfang von SMS Nachrichten am seriellen Anschluss freizugeben.

Durch die Auswahl der Option *Enable AT-SMS Protocol on TCP Port* ist es möglich, das Versenden / den Empfang von SMS Nachrichten am TCP Anschluss freizugeben. Die SMS Nachrichten werden mittels der standardmäßigen AT Befehle versandt. Mehr über AT finden Sie in **[1]**.

Die Optionen *Enable AT-SMS Protocol on External Port* und *Enable AT-SMS Protocol on TCP Port* dürfen nicht gleichzeitig angekreuzt werden.

SMS Configuration

- [ ] Send SMS on power up
- [ ] Send SMS on PPP connect
- [ ] Send SMS on PPP disconnect
- [ ] Send SMS when datalimit is exceeded
- [ ] Send SMS when binary input is active

Phone Number 1
Phone Number 2
Phone Number 3
Unit ID *
BIN1 - SMS *
BIN2 - SMS *
BIN3 - SMS *
BIN4 - SMS *

- [x] Enable remote control via SMS

Phone Number 1
Phone Number 2
Phone Number 3

- [ ] Enable AT-SMS protocol on expansion port

Baudrate 9600

- [ ] Enable AT-SMS protocol over TCP

TCP port
** can be blank*

Apply

Nach dem Einschalten der Stromversorgung (Power Up) kommen an die angeführten Telefonnummern die SMS im Format an:

ER 75i (Unit ID) has been powered up. PLMN:xxxxx,Cell:xxxx,Channel:xx,Level:-xx dBm,

wobei PLMN – Netzbetreibernummer, Cell – Zellennummer, Channel – angewandter Kanal, Level – Signalpegel bedeuten

Nach dem Aufbau der PPP Verbindung (PPP Connect) kommen an die angeführten Telefonnummern die SMS im Format an:

ER 75i (Unit ID) has established PPP connection. IP address xxx.xxx.xxx.xxx

Nach der Auflösung der PPP Verbindung (PPP Disconnect)kommen an die angeführten Telefonnummern die SMS im Format an:

ER 75i (Unit ID) has lost PPP connection. IP address xxx.xxx.xxx.xxx

LUCOM GmbH * Ansbacher Str. 2a * 90513 Zirndorf * Tel. 09127/59 460-10 * Fax. 09127/59 460-20 * www.lucom.de

Die Einstellung des Versendens von diesen SMS ist, wie folgt:

SMS Configuration

- [x] Send SMS on power up
- [x] Send SMS on PPP connect
- [x] Send SMS on PPP disconnect
- [x] Send SMS when datalimit is exceeded
- [x] Send SMS when binary input is active

Phone Number 1	723123456
Phone Number 2	732123456
Phone Number 3	721123456
Unit ID *	Router
BIN1 - SMS *	Bin1
BIN2 - SMS *	Bin2
BIN3 - SMS *	Bin3
BIN4 - SMS *	Bin4

- [x] Enable remote control via SMS

Phone Number 1	
Phone Number 2	
Phone Number 3	

- [ ] Enable AT-SMS protocol on expansion port

Baudrate	9600

- [ ] Enable AT-SMS protocol over TCP

TCP port	

** can be blank*

Apply

Beispiel für die Routereinstellung zum Versand von SMS Nachrichten über die serielle Schnittstelle:

SMS Configuration

- [ ] Send SMS on power up
- [ ] Send SMS on PPP connect
- [ ] Send SMS on PPP disconnect
- [ ] Send SMS when datalimit is exceeded
- [ ] Send SMS when binary input is active

Phone Number 1
Phone Number 2
Phone Number 3
Unit ID *
BIN1 - SMS *
BIN2 - SMS *
BIN3 - SMS *
BIN4 - SMS *

- [ ] Enable remote control via SMS

Phone Number 1
Phone Number 2
Phone Number 3

- [x] Enable AT-SMS protocol on expansion port

Baudrate 9600

- [ ] Enable AT-SMS protocol over TCP

TCP port
** can be blank*

Apply

Mit den SMS Nachrichten ist es möglich, z. B. im Programm Hyperterminal zu arbeiten. Nach dem Aufbau der Verbindung mit dem Router über die serielle Schnittstelle oder Ethernet ist es möglich mittels der folgenden AT Befehle mit den SMS Nachrichten zu arbeiten (mehr AT Befehle in der Literatur **[1]**):

AT Befehle	Bedeutung
AT+CMGF=1	Einstellung vom Textmodus zum Schreiben der SMS Nachrichten
AT+CMGS="Telefonnummer"	Der Befehl gibt die Möglichkeit, die SMS an die angeführte Telefonnummer zu senden
AT+CMGL=ALL	Einlesen der Liste von allen SMS Nachrichten
AT+CMGR=<index>	Lesen von einer bestimmten SMS Nachricht (alle SMS haben ihren eigenen Index)
AT+CMGD=<index>	Löschen der SMS in Abhängigkeit vom Nachrichtindex

Zum Einstellen des Schreibens einer SMS Nachricht im Textmodus wird der Befehl *AT+CMGF=1* angewandt.

AT+CMGF=1 Enter

OK

Die Textnachricht wird mittels des Befehls *AT+CMGS=<Telefonnummer>* erstellt. Nach der Betätigung der *Enter* Taste wird das Zeichen > angezeigt, dahinter kann der eigene Text der SMS Nachricht geschrieben werden. Nach dem Verfassen der SMS wird die

Tastenkombination *CTRL+Z zum Versenden* verwendet (das Versenden der SMS Nachricht dauert einige Zeit). Das Verfassen der Nachricht wird mit der Taste *Esc* aufgehoben.

AT+CMGS="712123456" Enter

>***Hello World!*** CTRL+Z (Tastenkombination)

OK

Mit dem Befehl *AT+CMGL=ALL ist es möglich, eine neue SMS* zu ermitteln. Mit diesem Befehl werden alle SMS Nachrichten eingelesen.

AT+CMGL=ALL Enter

+CMGL: <Index>, <Status>,<Absendernummer>, <Datum>,<Zeit>
Text der SMS Nachricht.

+CMGL: 1,"REC UNREAD","+420721123456", ,"08/02/02, 10:33:26+04"
Hello World!

wo <Index> die laufende Nummer der SMS Nachricht ist,

<Status> der Zustand der SMS Nachricht ist:

REC UNREAD – SMS Nachricht nicht gelesen
REC READ – SMS Nachricht gelesen
STO UNSENT – gespeicherte, nicht abgesandte SMS Nachricht
STO SENT – gespeicherte abgesandte SMS Nachricht
ALL – alle SMS Nachrichten

<Absendernummer> ist die Telefonnummer, von der die SMS Nachricht empfangen wurde,

<Datum> das Datum des SMS Empfangs ist,

<Zeit> die Zeit des SMS Empfangs ist.

Die neue SMS Nachricht ist es möglich, mit dem Befehl AT+CMGR=<Index> zu lesen.

AT+CMGR=1 Enter

+CMGL: <Index>, <Status>,<Absendernummer>, <Datum>,<Zeit>
Text der SMS Nachricht.

+CMGL: 1,"REC READ","+420721123456", ,"08/01/12, 9:48:04+04"
Hello World!

Die empfangene SMS Nachricht kann mit dem Befehl AT+CMGD=<Index> gelöscht werden.

AT+CMGD=1 Enter

OK

4.20. Konfiguration des Erweiterungsanschlusses PORT1

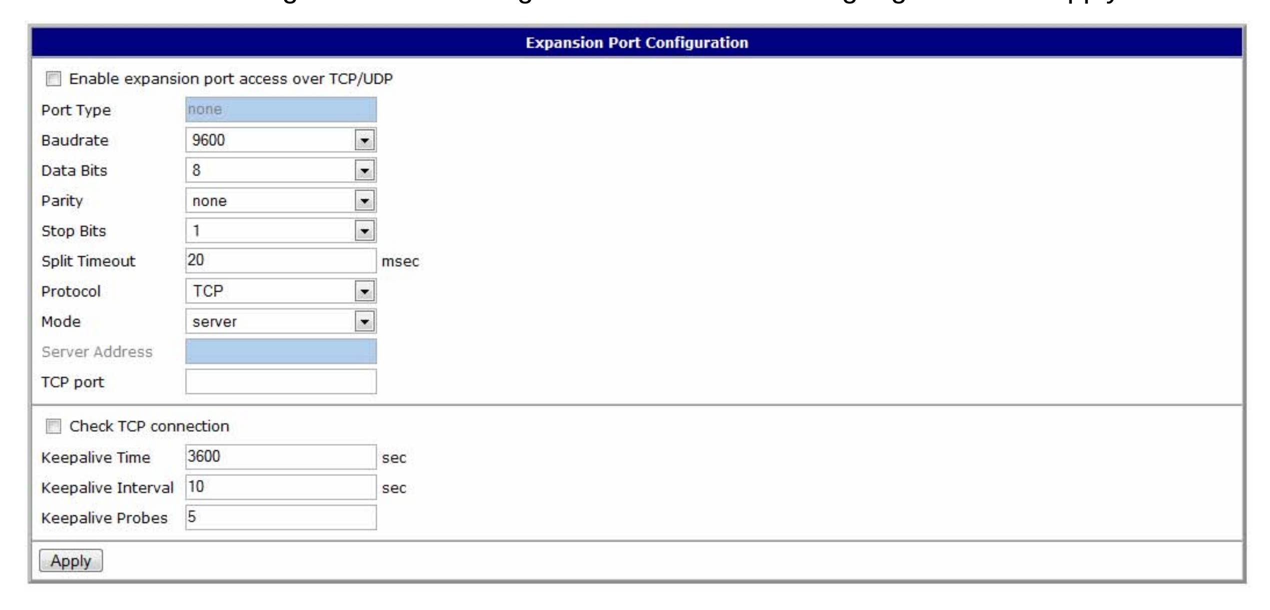
Die Konfiguration des Erweiterungsanschlusses PORT1 kann durch die Auswahl der Option External Port im Menü aufgerufen werden. Im Fenster können die Geschwindigkeit der Kommunikation (*Baudrate*), die Anzahl der Datenbits (*Data Bits*), die Parität (*Parity*), die Anzahl der Stoppbits (*Stop Bits*), das Protokoll (*Protocol*) definiert und der Modus der Tätigkeit (*Mode*) gewählt werden.

Split Timeout stellt die Zeit für die Zerteilung der Nachricht ein. Wird beim Empfang eine Lücke zwischen zwei Zeichen, die länger als der Wert des Parameters in Millisekunden ist, erkannt, wird der Empfang als fehlerhaft angezeigt und es folgt das Aufsuchen vom neuen Anfang der Nachricht.

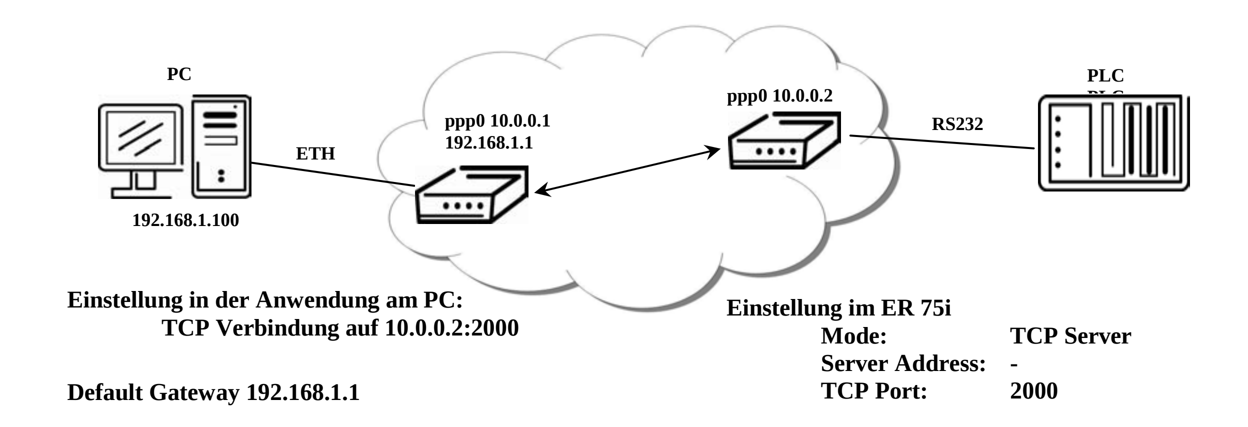
Im Modus des TCP Servers ist es notwendig, den TCP Anschluss einzugeben, an dem der Router die ankommenden Anforderungen auf TCP Verbindung anhört. Im Modus des TCP Klienten ist es notwendig die Serveradresse und den TCP Zielanschluss einzugeben.

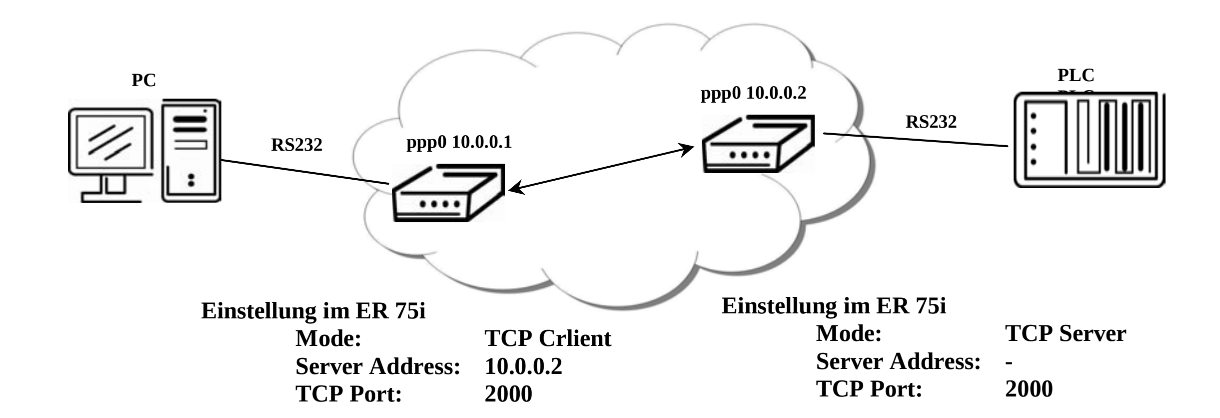
Ist die Option *Check TCP Connection* angekreuzt, wird die Kontrolle der aufgebauten TCP Verbindung aktiviert. Im Fenster können die Zeit, nach der die Kontrolle der Verbindung erfolgt (*Keepalive Time*), die Zeit der Antwortabwartung (Keepalive Interval) und die Versuchsanzahl (*Keepalive Probes*) definiert werden.

Die Änderungen der Einstellung wirken sich nach Betätigung der Taste Apply aus.



Beispiel für die Konfiguration des Erweiterungsanschlusses:



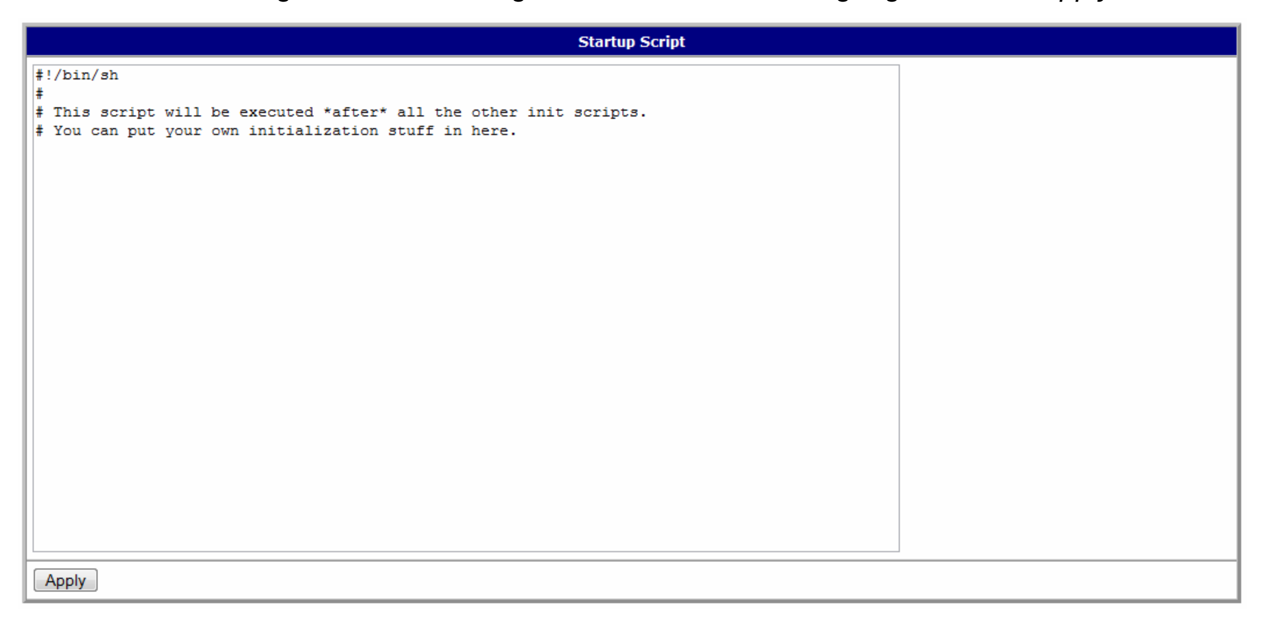




4.21. Konfiguration des Startskripts

Im Fenster *Startup Script* ist es möglich eigene Skripten zu erstellen, die nach den Initialisierungsskripten gestartet werden. Bei der Erstellung der Sicherheitskopie sowie bei der Wiederherstellung der Konfiguration werden weder Sicherheitskopien der Skripten erzeugt, noch die Skripten wiederhergestellt.

Die Änderungen der Einstellung wirken sich nach Betätigung der Taste *Apply* aus.



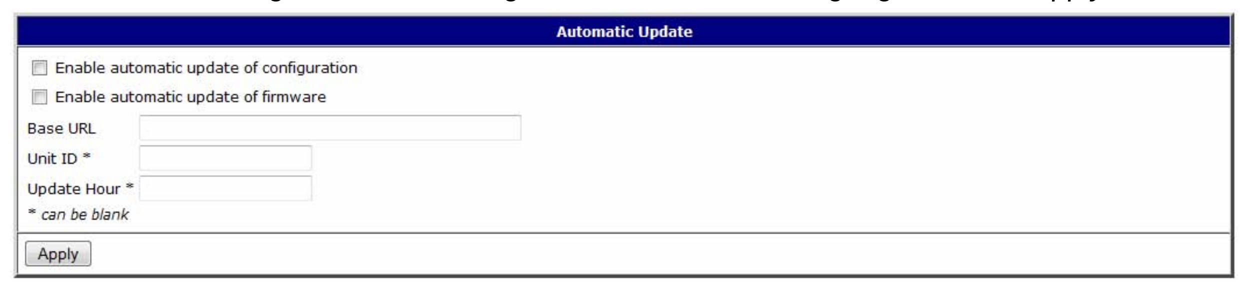
4.22. Konfiguration der automatischen Aktualisierung der Einstellungen

Die Konfiguration der automatischen Aktualisierung der Routereinstellungen kann im Menü durch die Auswahl der Option *Automatic Update* aufgerufen werden. Diese Option ermöglicht, dass der Router selbst die Konfiguration oder die aktuelle Firmware vom Server, wo die Konfiguration oder die Firmware gespeichert wird, automatisch herunterlädt.

Durch das Ankreuzen der Option *Enable Automatic Update of Configuration* ist es möglich die automatische Aktualisierung der Routereinstellungen freizugeben. Mit dem Parameter *Enable automatic update of firmware* ist es möglich die automatische Aktualisierung der Router-Firmware freizugeben. Mit dem Parameter *Base URL* ist es möglich, den Grundteil der Domäne oder IP Adresse einzugeben, von der die Routerkonfiguration heruntergeladen wird. Diese Adresse wird dann mit dem Inhalt des Parameters *Unit ID*, oder wenn das Feld *Unit ID* nicht ausgefüllt ist, mit der MAC Adresse ergänzt. Die Bezeichnung der heruntergeladenen Datei setz sich aus dem Parameter *Base URL*, der Hardwareadresse MAC der ETH0 Schnittstelle des Routers und aus dem Suffix *cfg* zusammen. Die Hardwareadresse MAC und das Suffix *cfg* werden automatisch hinzugefügt, es ist nicht erforderlich, diese Daten irgendwo auszufüllen. Mit dem Parameter *Unit ID* kann die sachliche Bezeichnung der heruntergeladenen Datei definiert werden, die auf den Router heruntergeladen wird. Falls dieser Parameter verwendet wird, wird die Hardwareadresse MAC in der Bezeichnung der heruntergeladenen Datei nicht benutzt.

Die automatische Aktualisierung der Konfiguration erfolgt 5 Minuten nach dem Einschalten des Routers und dann alle 24 Stunden, oder es ist möglich mit dem Parameter Update Hour die Stunde (im Bereich von 1–24) einzustellen, wann die Aktualisierung durchzuführen ist. Besteht an der eingegebenen URL eine abweichende Konfiguration als im Router, nimmt der Router diese Konfiguration auf und danach führt er einen erneuten Start durch.

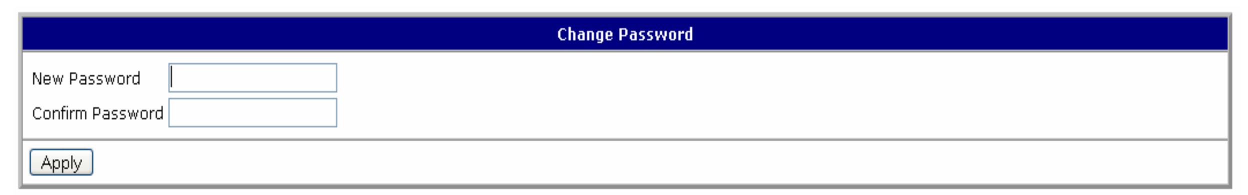
Die Änderungen der Einstellung wirken sich nach Betätigung der Taste *Apply* aus.



4.23. Änderung des Zutrittspasswortes

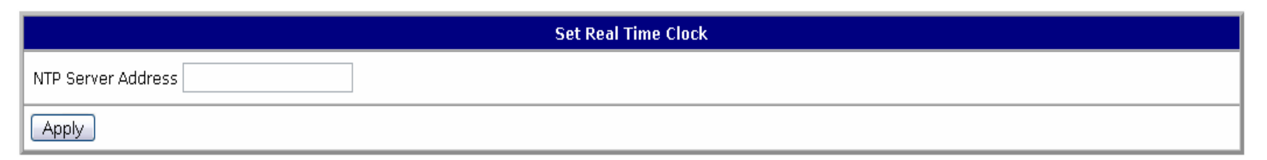
Das Dialogfenster zur Passwortänderung kann durch die Auswahl der Option *Change Password* im Menü aufgerufen werden. Das neue Passwort wird nach der Betätigung der Taste *Apply* gespeichert.

In der Grundeinstellung des Routers ist das Passwort auf die Ausgangsform *root* eingestellt. Um die höhere Sicherheit des vom Router verwalteten Netzes sicherzustellen, wird empfohlen dieses Passwort zu ändern.



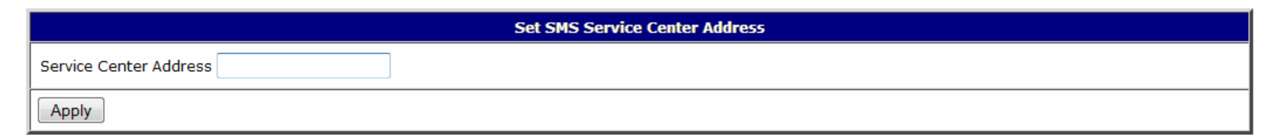
4.24. Einstellung der internen Uhr

Die einmalige Einstellung der internen Routeruhr kann durch die Auswahl der Option *Set Real Time Clock* im Menü aufgerufen werden. Die Uhr wird in Abhängigkeit vom eingegebenen NTP Server nach der Betätigung der Taste *Apply*, z. B. *ntp.nic.cz* eingestellt.



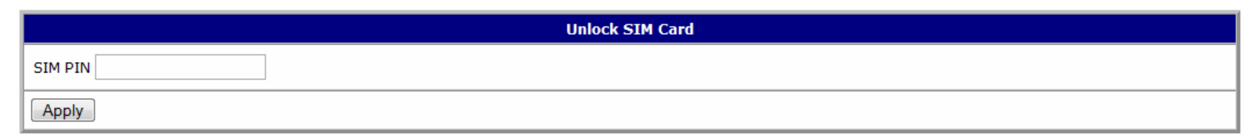
4.25. Einstellung des SMS Zentrums

In einigen Fällen ist es notwendig die Telefonnummer vom SMS Zentrum einzustellen, um die SMS Benutzernachrichten auszusenden. Der Parameter muss bei den SIM Karten, die die Telefonnummer des SMS Zentrums vom Netzbetreiber eingestellt haben, nicht eingestellt werden. Die Telefonnummer kann ohne der internationalen Vorwahl xxx xxx xxx oder mit der internationalen Vorwahl +420 xxx xxx xxx angeführt werden.



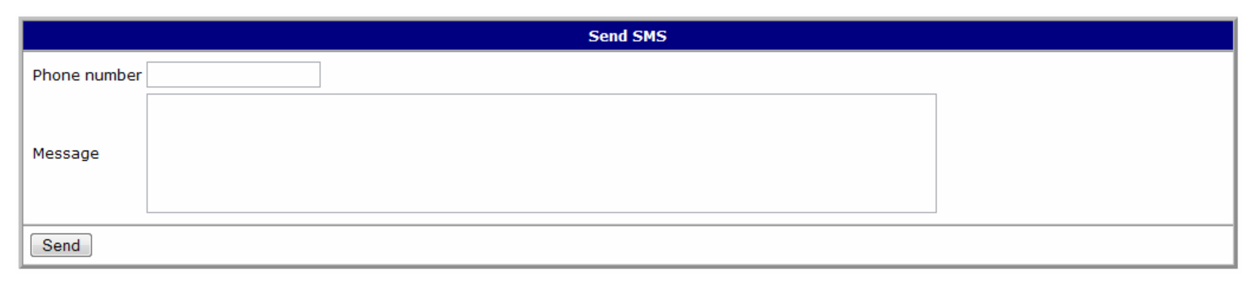
4.26. Erschließung der SIM Karte mittels PIN

Die Möglichkeit der Erschließung der SIM Karte ist unter der Option *Unlock SIM Card* angeführt. Ist die in den Router eingelegte SIM Karte mit einem PIN geschützt, wird der PIN (vierstellige Nummer) in das Feld *SIM PIN* eingetragen, die SIM Karte wird durch das Anklicken der Taste Apply erschlossen.



4.27. Versenden einer SMS Nachricht

Das Versenden einer SMS Nachricht ist im Fenster *Send SMS* möglich. Nach der Eingabe der Telefonnummer des Empfängers (*Phone Number*) sowie des Textes der SMS Nachricht (*Message*) wird die Nachricht mit der Taste *Send* abgesandt.



Versenden der SMS Nachricht über die HTTP Abfrage ist dann im Format:

GET /send_exec.cgi?phone=%2B**420712345678**&message=**Test** HTTP/1.1
Authorization: Basic cm9vdDpyb290

Die HTTP Abfrage wird in die TCP Verbindung am Anschluss 80 des Routers gesandt, der anschließend eine SMS im Format Test an die eingegebene Nummer 420712345678 sendet. Die Autorisierung ist im Format „User:Password" verschlüsselte BASE64, das Beispiel ist für root:root.

4.28. Erstellung der Sicherheitskopie der Konfiguration

Es ist möglich die Modemkonfiguration mittels der Option *Backup Configuration* zu speichern. Nach dem Anklicken ist es möglich das Zielverzeichnis auszuwählen, wo die Konfigurationsdatei des Routers gespeichert wird.

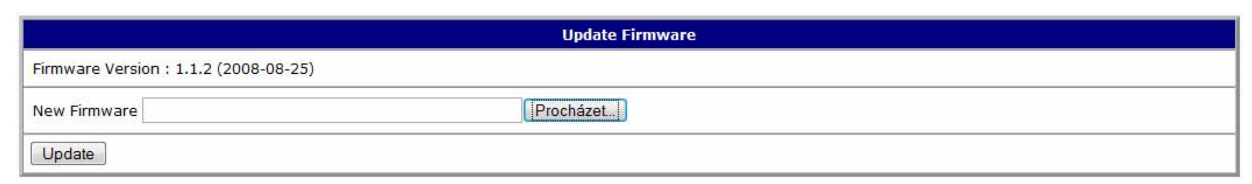
4.29. Wiederherstellung der Konfiguration

Falls die Router Konfiguration wieder herhergestellt werden soll, ist es möglich die Konfigurationsdatei in der Option *Restore Configuration* mittels der Taste *Durchsuchen* zu wählen.

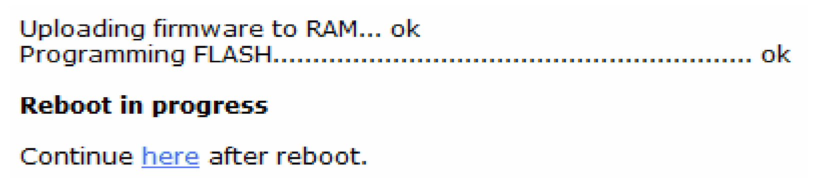


4.30. Aktualisierung der Firmware

Informationen über die Firware-Version und die Anweisungen zur Aktualisierung können durch die Auswahl der Option Update Firmware im Menü aufgerufen werden. Die neue Firmware wird in der Option *Durchsuchen* eingelesen und wird durch die anschließende Betätigung der Taste *Update* aktualisiert.



Nach erfolgreicher Aktualisierung der Firmware wird der folgende Auszug ausgeschrieben.

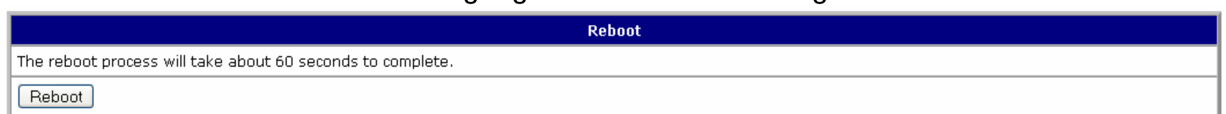


Dieser Auszug informiert über die Programmierung des FLASH Speichers.

Bei der Aktualisierung der Firmware ab Version 1.1.1 bleiben sämtliche Einstellungen samt der IP Adresse erhalten. Bei der Aktualisierung älterer Firmware als der Version 1.1.1 wird die eigene Router-Adresse auf 192.168.1.1 eingestellt (ein Verweis wird hier angeboten) und sämtliche Werte werden auf die Ausgangswerte eingestellt. Die Gesamtzeit der Aktualisierung beträgt etwa drei Minuten. Im Verlauf der Aktualisierung der Firmware muss eine ununterbrochene Stromversorgung sichergestellt werden. Die Fernaktualisierung wird mit Rücksicht auf die GPRS Verbindung nicht empfohlen, es könnte zur Beschädigung des Routers kommen.

4.31. Restart

Der erneuter Start des Routers kann durch die Auswahl der Option Reboot im Menü und durch die anschließende Betätigung der Taste *Reboot* aufgerufen werden.

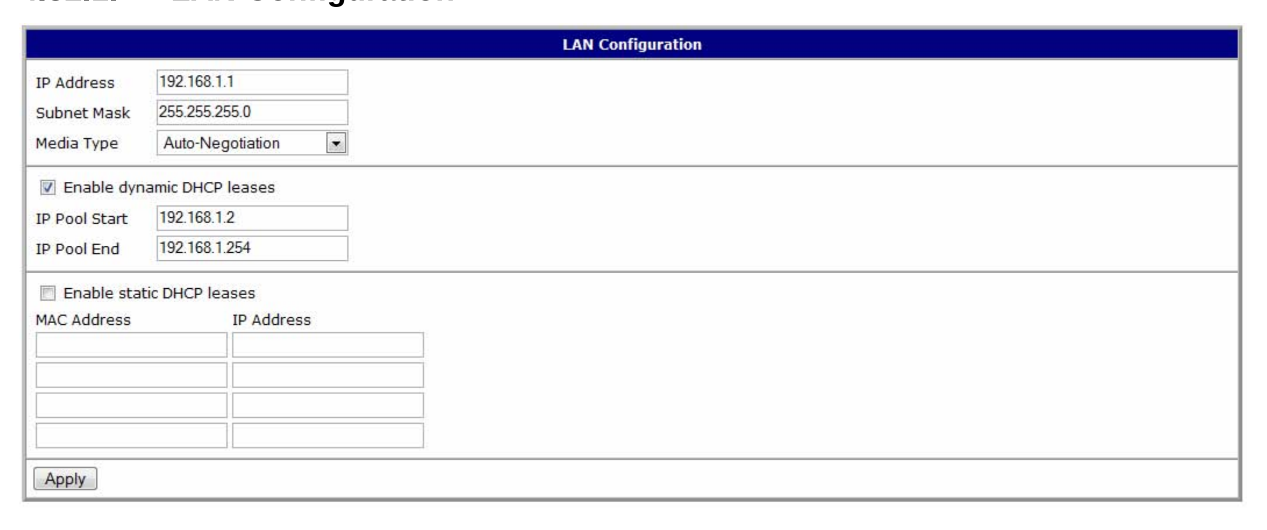




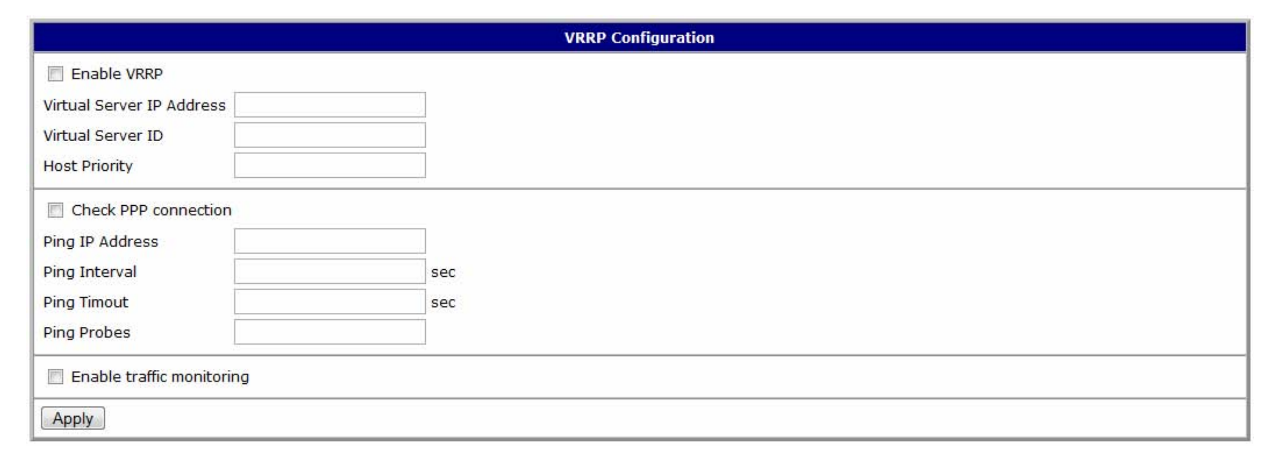


4.32. Standardeinstellung (Parameter des Herstellerwerkes)

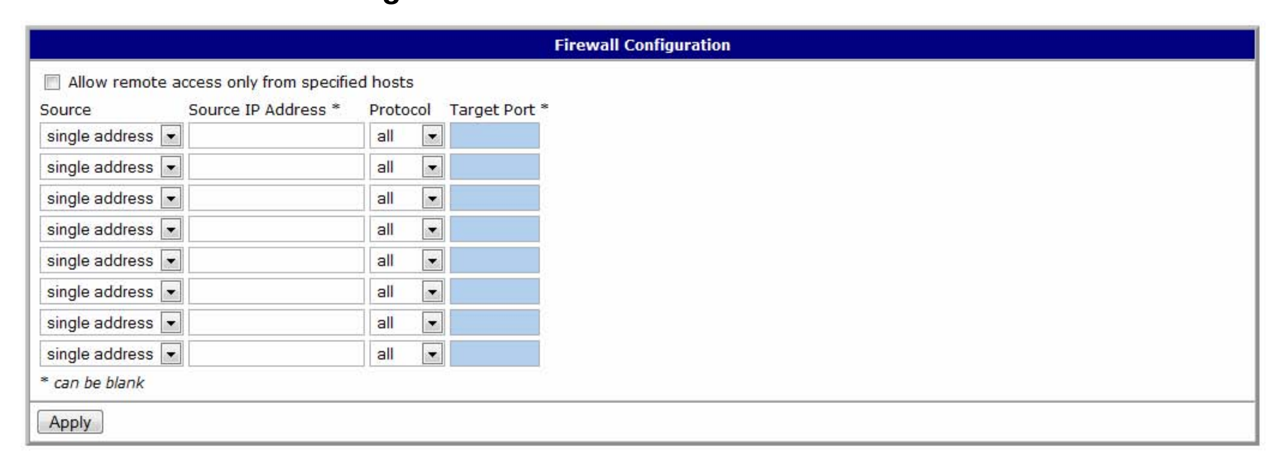
4.32.1. LAN Configuration



4.32.2. VRRP Configuration



4.32.3. Firewall Configuration



4.32.4. GPRS Configuration

GPRS Configuration

☑ Create PPP connection

	Primary SIM card	Secondary SIM card	
APN *			
Username *			
Password *			
IP Address *			
Operator *			
PIN *			
MRU	1500	1500	bytes
MTU	1500	1500	bytes

☑ Get DNS addresses from operator

☐ Check PPP connection (*necessary for uninterrupted operation*)

Ping IP Address			
Ping Interval			min

☐ Enable traffic monitoring

Data Limit		MB
Warning Threshold		%
Accounting Start	1	

Default SIM card	primary
Backup SIM card	secondary

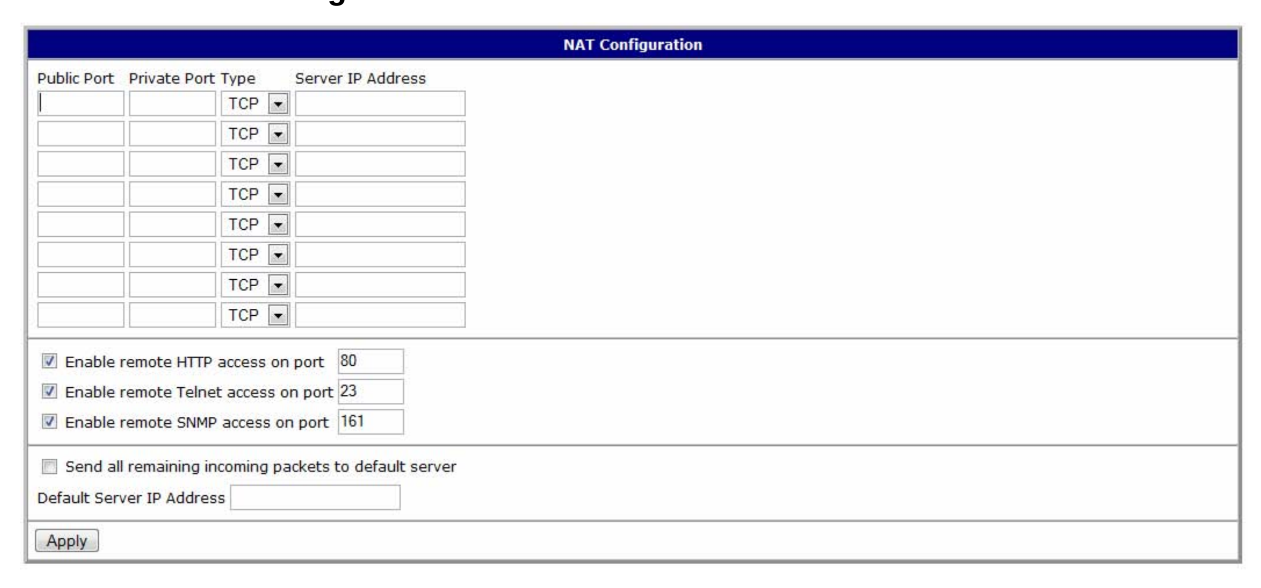
☐ Switch to other SIM card when connection fails
☐ Switch to backup SIM card when roaming is detected
☐ Switch to backup SIM card when data limit is exceeded
☐ Switch to primary SIM card after timeout

Initial Timeout	60	min
Subsequent Timeout *		min
Additive Constant *		min

** can be blank*

Apply

4.32.5. NAT Configuration



NAT Configuration

Public Port	Private Port	Type	Server IP Address
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	
		TCP	

☑ Enable remote HTTP access on port 80
☑ Enable remote Telnet access on port 23
☑ Enable remote SNMP access on port 161

☐ Send all remaining incoming packets to default server
Default Server IP Address

Apply

4.32.6. OpenVPN Tunnel Configuration

OpenVPN Tunnel Configuration

☐ Create OpenVPN tunnel

Protocol	UDP	
UDP port	1194	
Remote IP Address *		
Remote Subnet *		
Remote Subnet Mask *		
Redirect Gateway	no	
Local Interface IP Address		
Remote Interface IP Address		
Ping Interval *		sec
Ping Timeout *		sec
Renegotiate Interval *		sec
Max Fragment Size *		bytes
Compression	LZO	
NAT Rules	not applied	
Authenticate Mode	none	
Pre-shared Secret		
CA Certificate		
DH Parameters		
Local Certificate		
Local Private Key		
Username		
Password		

** can be blank*

Apply

4.32.7. IPsec Tunnel Configuration

IPsec Tunnel Configuration

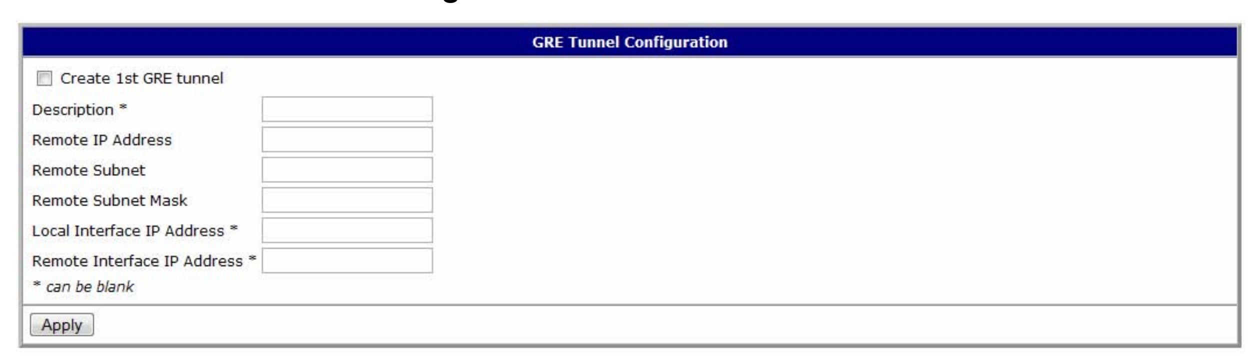
☐ Create 1st IPsec tunnel

Description *		
Remote IP Address *		
Remote ID *		
Remote Subnet *		
Remote Subnet Mask *		
Local ID *		
Local Subnet *		
Local Subnet Mask *		
Key Lifetime	3600	sec
IKE Lifetime	3600	sec
Rekey Margin	540	sec
Rekey Fuzz	100	%
NAT Traversal	disabled	
Aggressive Mode	disabled	
Authenticate Mode	pre-shared key	
Pre-shared Key		
CA Certificate		
Remote Certificate		
Local Certificate		
Local Private Key		
Local Passphrase *		

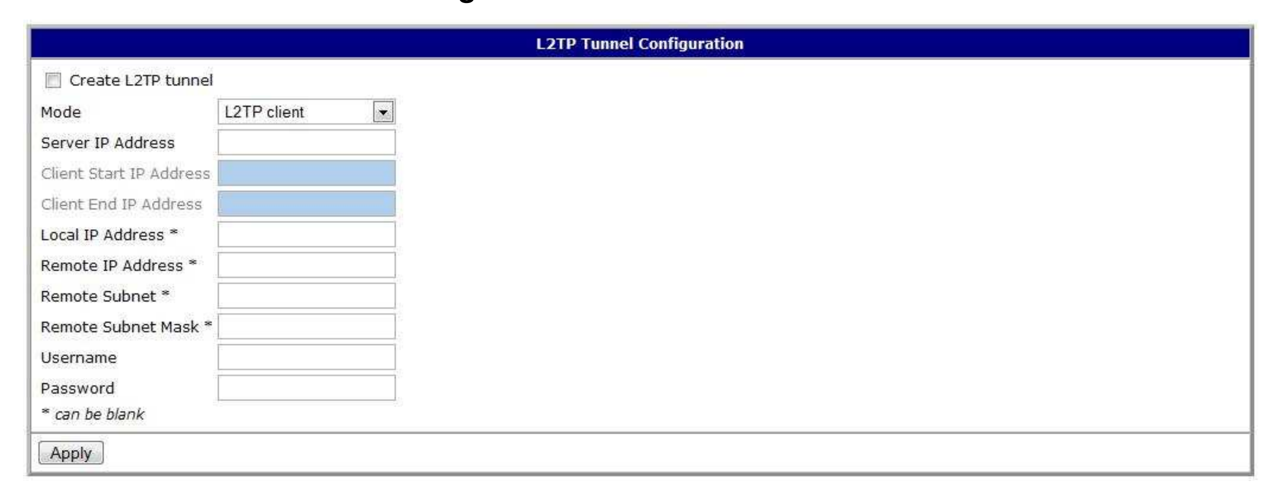
** can be blank*

Apply

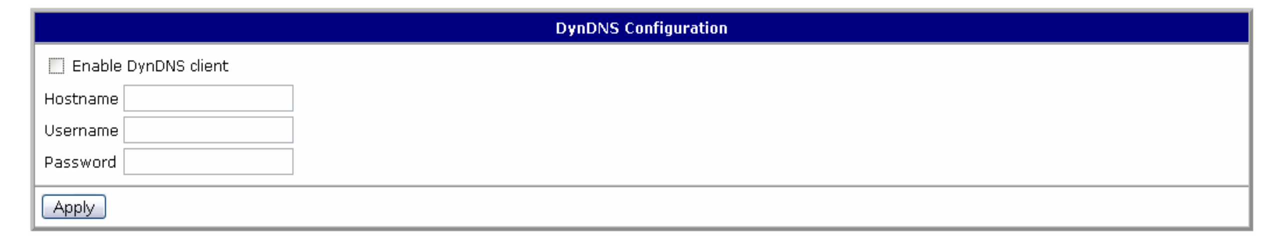
4.32.8. GRE Tunnel Configuration



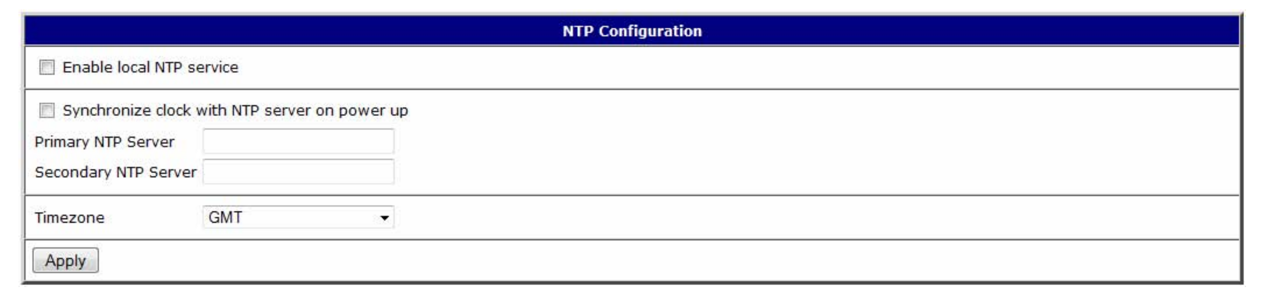
4.32.9. L2TP Tunnel Configuration



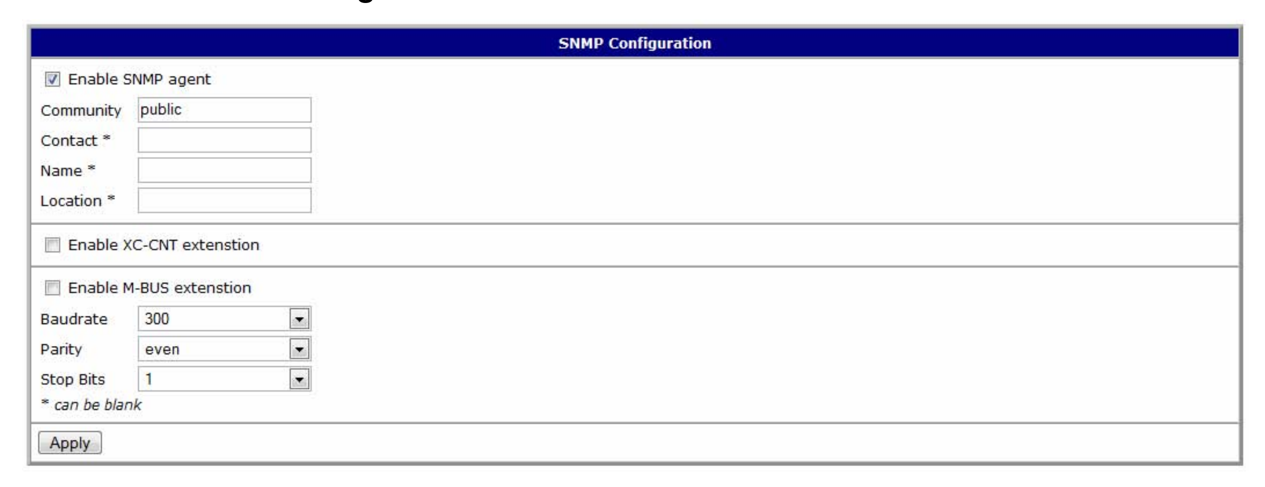
4.32.10. DynDNS Configuration



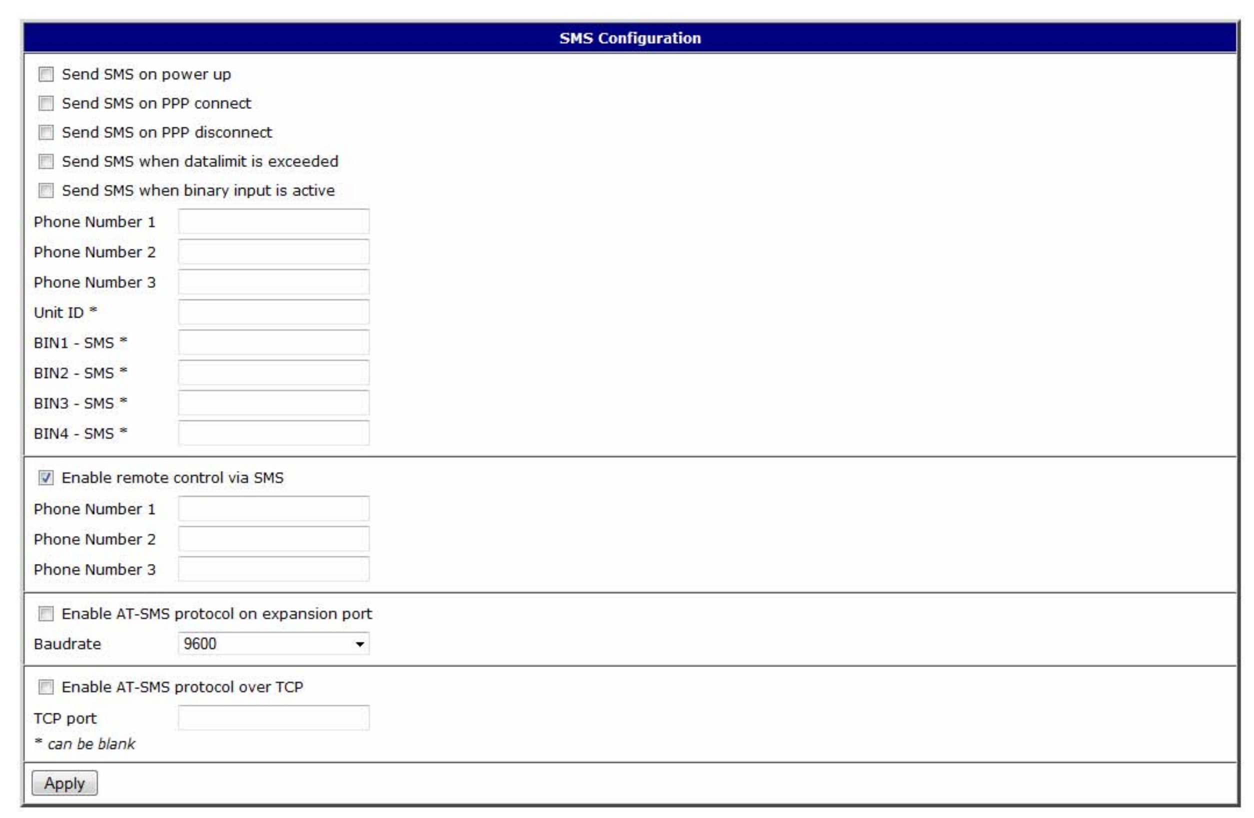
4.32.11. NTP Configuration



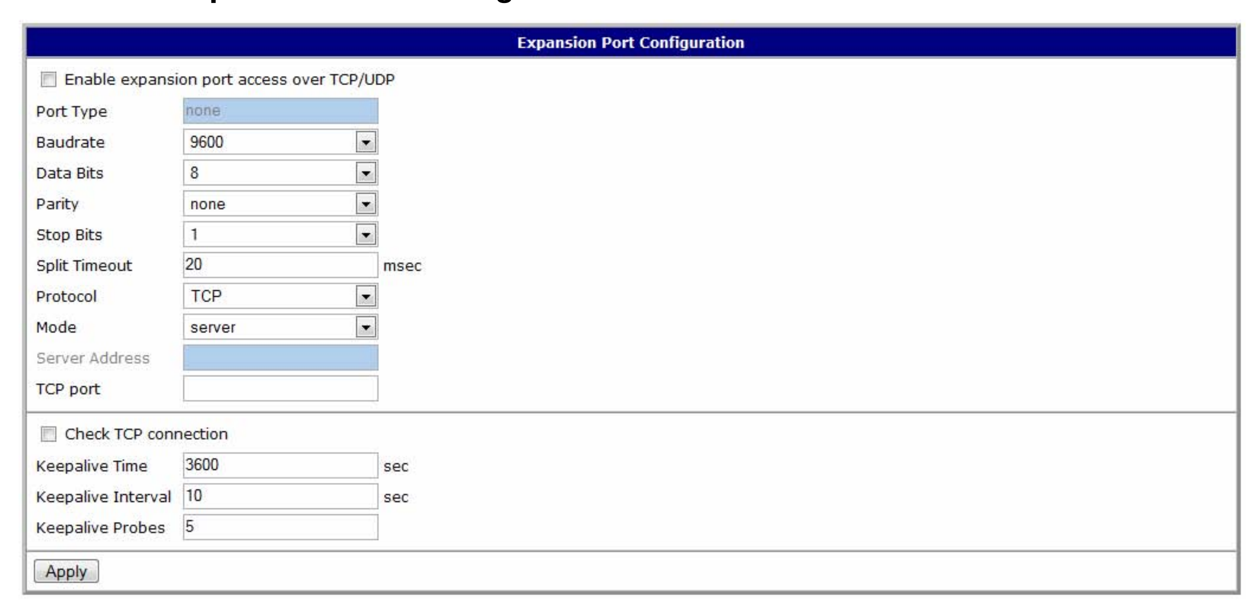
4.32.12. SNMP Configuration



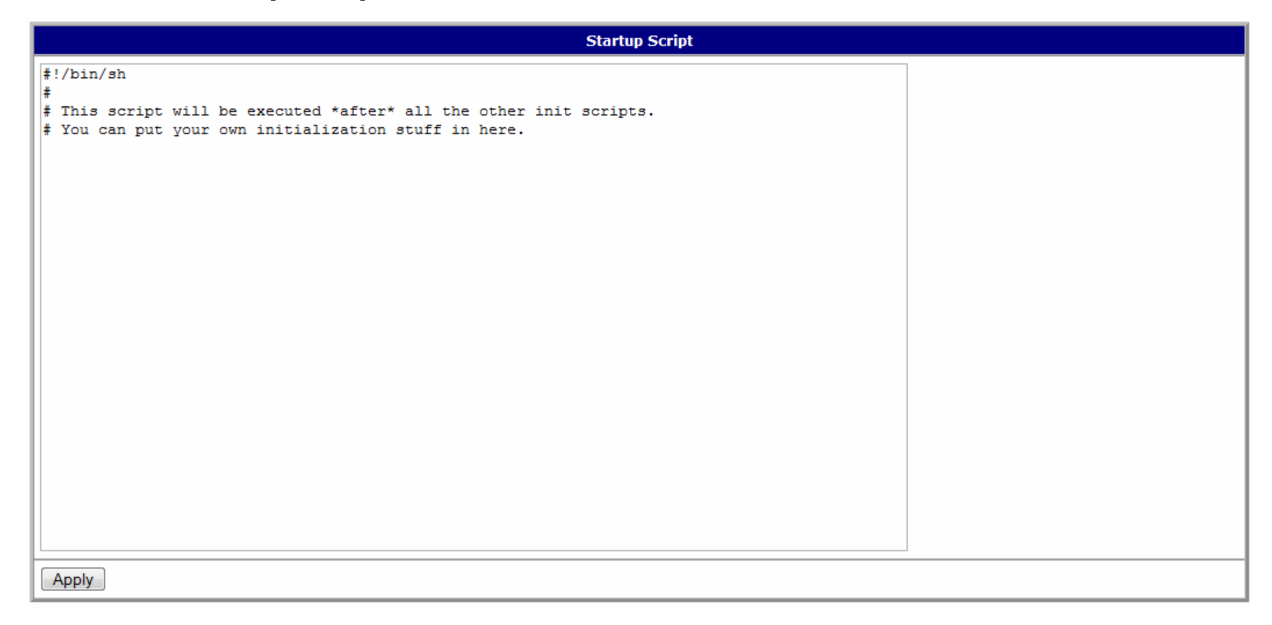
4.32.13. SMS Configuration



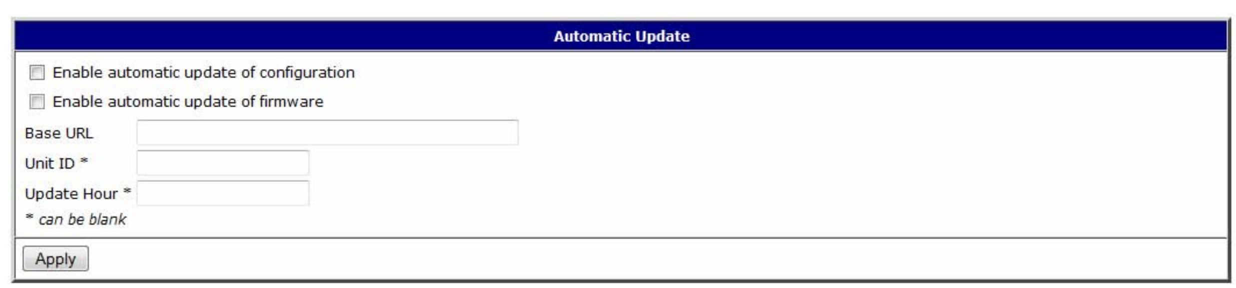
4.32.14. Expansion Port Configuration



4.32.15. Startup Script



4.32.16. Automatic Update



5. Einstellung der Konfiguration über Telnet



Vorsicht! Ohne eingelegte SIM Karte kann der Router nicht betrieben werden. Die eingelegte SIM Karte muss die GPRS Übertragungen aktiviert haben. Die SIM Karte legen Sie nur dann ein, wenn der Router abgeschaltet ist.

Zur Zustandsüberwachung, Konfiguration und Verwaltung des Routers steht die Telnet Schnittstelle zur Verfügung. Nach der Eingabe der IP Adresse des Routers in die Telnet Schnittstelle ist es möglich, die Konfiguration mittels der Befehle durchzuführen. Die IP Ausgangsadresse des Routers lautet 192.168.1.1. Die Konfiguration kann nur der Benutzer „root" mit dem Ausgangspasswort „root" vornehmen.

Für Telnet bestehen folgende Befehle:

Befehl	Beschreibung
cat	Auszug vom Dateiinhalt
cp	Datei kopieren
date	Anzeige / Änderung der Systemzeit
df	Anzeige der Informationen über das Dateisystem
dmesg	Anzeige der Diagnostikmeldungen von Kernel
echo	Auszug aus der Zeichenkette
free	Anzeige der Informationen über den Speicher
gsmat	Versand von AT Befehlen
gsminfo	Anzeige der Informationen über die Signalqualität
gsmsms	SMS Versand
hwclock	Anzeige / Änderung der Zeit im RTC Kreis
ifconfig	Anzeige / Änderung der Schnittstellenkonfiguration
ip	Anzeige / Änderung der Richttabelle
iptables	Anzeige / Anpassung der Regeln für den Net Filter
kill	Prozessunterbindung
killall	Prozessunterbindung
ln	Erstellung der Verknüpfung
ls	Auszug aus dem Verzeichnisinhalt
mkdir	Verzeichniserstellung
mv	Dateiverschiebung
ntpdate	Synchronisierung der Systemzeit mit dem NTP Server
passwd	Passwortänderung
ping	ICMP Ping
ps	Anzeige der Informationen über die Prozesse
pwd	Auszug aus dem aktuellen Verzeichnis
reboot	Restart
rm	Datei löschen
rmdir	Verzeichnis löschen
route	Anzeige / Änderung der Richttabelle
service	Dienststart / -stopp
sleep	Pause für die vorgegebene Sekundenanzahl
slog	Anzeige des Systems Log
tail	Anzeige des Dateiendes
tcpdump	Überwachung des Netzbetriebs

touch	Dateierstellung / Aktualisierung des Dateizeitstempels
vi	Texteditor

6. Treiberinstallation

Schließen Sie das USB Kabel an den Router und den PC an. Windows erfasst den Router als einen neuen USB Router, startet den *Assistenten zum Hinzufügen der neuen Hardware* und erfordert den Treiber für das Modul bzw. für „Siemens AG WM USB Modem” an. Befolgen Sie die Anweisungen des Assistenten und geben Sie den Pfad zur Datei „usbmodem.inf” ein. Windows kopiert die erforderlichen Dateien in Ihren Computer und konfiguriert den Router durch die Zuteilung eines freien COM Anschlusses. Nach der Beendigung des Kopierens der Dateien klicken Sie die Taste *Fertigstellen* an.

Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

Siemens AG WM USB Modem

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

Install the software automatically (Recommended)

Install from a list or specific location (Advanced)

Found New Hardware Wizard

Completing the Found New Hardware Wizard

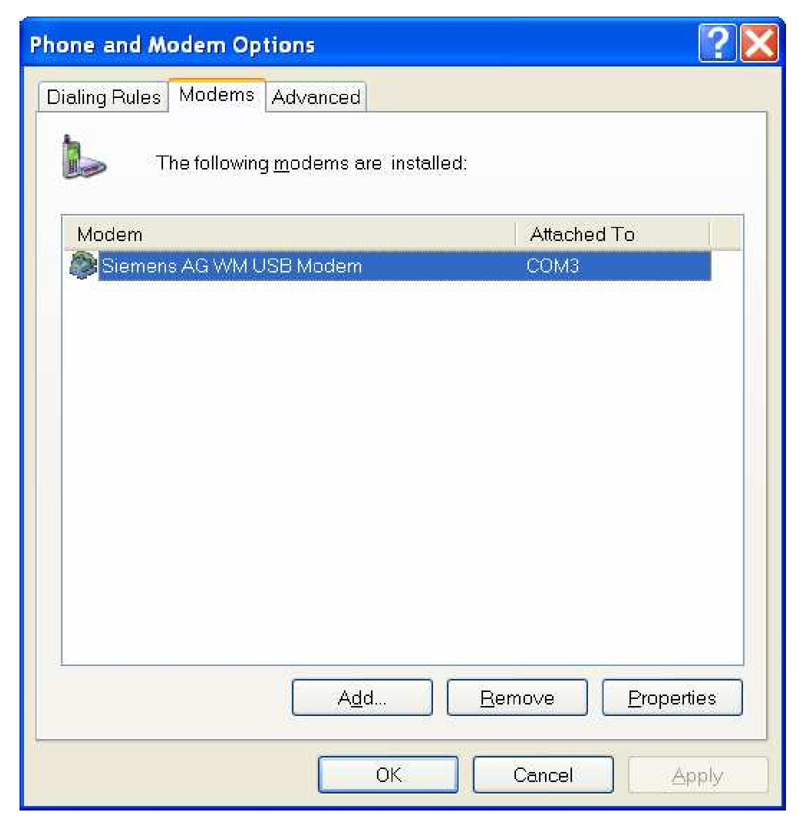
The wizard has finished installing the software for:

Siemens AG WM USB Modem

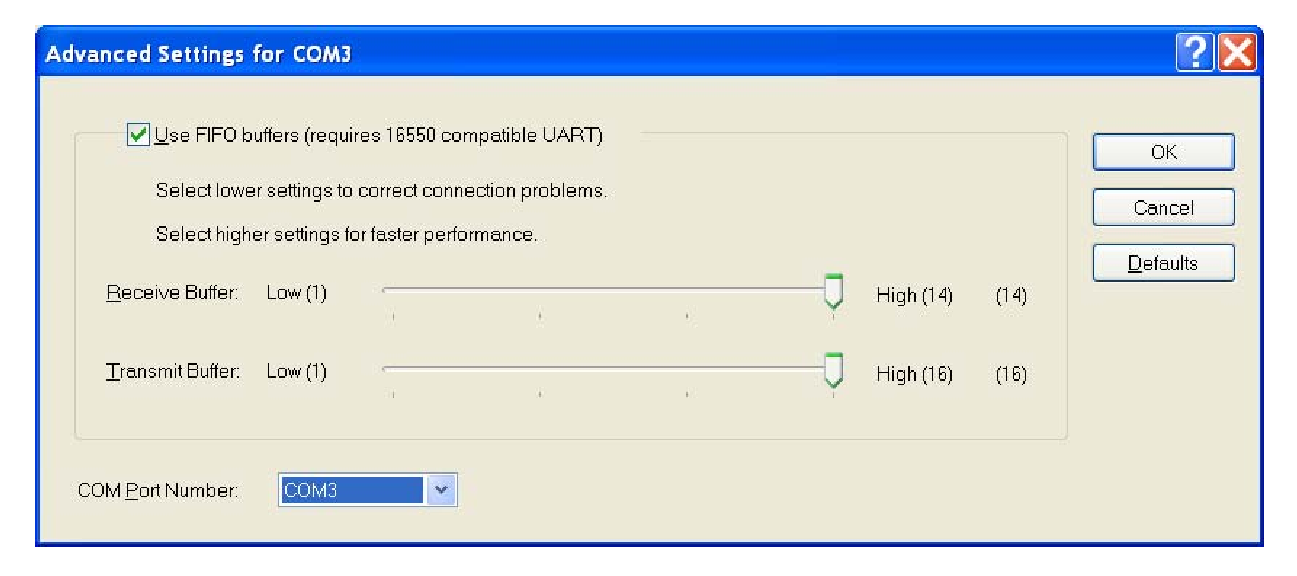
Click Finish to close the wizard.

< Back | Finish | Cancel

Den installierte Router finden Sie in der Systemsteuerung, Telefon und Modem Optionen (Start | Einstellungen | Systemsteuerung | Telefon und Modem Optionen| Modems).



Den zugeteilten COM Anschluss können Sie im Gerätemanager ändern. Im Menü der installierten Geräte wählen Sie „Siemens AG WM USB Modem" aus, klicken Sie die Eigenschaften an, wählen Sie die Karte Erweiterte Einstellungen aus und klicken Sie die Taste Feinabstimmung von Anschlusseinstellung an. In der Option *COM Anschlussnummer* wählen Sie dann den erwünschten freien COM Anschluss aus. Die Änderung der Einstellung des COM Anschlusses wirkt sich erst nach dem Herausnehmen und dem erneuten Anschluss des USB Kabels aus.





7. Betätigung mit AT Befehlen

Der Router wird mittels der AT Befehle betätigt und programmiert. Der Aufbau eines AT Befehls entspricht dem benutzten Modul MC75i. AT Befehle sind auf den Internetseiten http://www.siemens.de/wm zu finden.



8. Mögliche Probleme

Bei manchen Netzkarten kann es vorkommen, dass der Router nicht angeschlossen werden kann. Dieses Problem kann durch folgende Schritte gelöst werden:

- durch die manuelle Auswahl der Geschwindigkeit der Kommunikation von 10 MB/s in den Eigenschaften der Netzkarte,
- durch den Anschluss des Routers über Switch,
- durch das Starten des Computers erst nach dem Beenden des Startens des Routers.



9. Literatur

[1] Cinterion**: MC75i_ATC_V00.031 – AT Command Set, 2008**



10. FAQ (oft gestellte Fragen)

- Aus dem Internet kann ich das an den Router angeschlossene Gerät nicht erreichen und ich habe NAT eingestellt.
  - *Auf dem Gerät müssen Sie die Gateway auf den Router eingestellt haben.*
- Der Router führt ein Reset durch, die Verbindung im Ethernet fällt aus.
  - *Es ist notwendig, dass Sie eine Antenne im größeren Abstand vom Versorgungsnetzteil benutzen.*
- Ich kann den Webserver hinter NAT nicht erreichen.
  - *Sie müssen den http Fernzutritt auf dem Router verbieten, die Adresse des Ausgangsservers auf Ihren Webserver einstellten und auf dem Webserver die Gateway auf den Router einstellen.*
- Die GPRS Verbindung fällt aus.
  - *Überprüfen Sie die Signalstärke. Ist das Signal zu schwach, benutzen Sie eine bessere Antenne. Haben die Zellen in der näheren Umgebung ein ähnliches Signal, ist es notwendig eine Richtantenne zu benutzen. Die Signalstärke muss im Bereich zwischen -50 dBm und -90 dBm liegen.*
  - *Es ist erforderlich Ping einzustellen, damit wird die Verbindung kontrolliert und im Falle eines GPRS Ausfalls erneut aufgebaut.*
- Die GPRS Verbindung wird nicht aufgebaut.
  - *Überprüfen Sie die Einstellung gprs – APN, Name, Passwort und IP Adresse.*
  - *Versuchen Sie den PIN einzugeben – Kontrollieren Sie, ob die SIM Karte nicht den PIN Code eingestellt hat.*
  - *Bei privaten APN ist es geeignet, das Versenden von DNS Servern abzuschalten.*
  - *Schalten Sie das System Log ein und beobachten Sie, wo ein Fehler auftritt.*

- Die Verbindung im Ethernet fällt aus oder wird nicht aufgebaut.
  - *An der Ethernet Schnittstelle des Routers kann die Autonegotiation abgeschaltet werden und die Geschwindigkeit und der Duplex lassen sich manuell einstellen.*
- Wie sind die AT Befehle einzugeben?
  - *Sie müssen den USB Anschluss zu benutzen. Vorsicht, es nicht möglich gleichzeitig die GPRS Verbindung vom Router aus aufzubauen.* DynDNS funktioniert nicht.
  - *Im privaten APN funktioniert es nicht.*
  - *Sind die gleiche IP Adresse bei Ihrem kanonischen Namen und die dynamisch zugeteilte Adresse aufgezeichnet, bedeutet es, dass der Netzbetreiber NAT oder Firewall benutzt.*
  - *NAT kann durch Ping an die Adresse von Ihrem beliebigen Server mit einer festen IP Adresse und durch die Kontrolle der Adressen des Routers und der Adresse in Ping überprüft werden.*
  - *Die Firewall kann zum Beispiel per Fernzutritt auf die Webschnittstelle überprüft werden.*
  - *Der Netzbetreiber teilt die Adresse der DNS Server nicht zu und ohne DNS Server ist es nicht möglich die Verbindung zum Server dyndns.org aufzubauen. Im System Log wird diese Nachricht abgebildet:*
    - DynDNS daemon started
    - Error resolving hostname: no such file or directory
    - Connect to DynDNS server failed
- IPsec Tunnel wird aufgebaut, jedoch die Kommunikation funktioniert nicht.
  - *Wahrscheinlich sind die Richtregeln der angeschlossenen Geräte oder der Gateway falsch eingestellt.*
- Die FTP Verbindung funktioniert nicht.
  - *ER 75i unterstützt nur den passive FTP Modus, d. h. dass der Server dem Klienten den Anschluss (mehr als 1024) sendet und der Klient schließt sich daran an (z > 1024).*
- RS232 funktioniert nicht.
  - *Es ist notwendig, das Vorhandensein der Erweiterungsplatte RS232 zu überprüfen.*
  - *Überprüfen Sie das Vorhandensein der Platte in der Router Konfiguration auf der Karte „External Port“, oder überprüfen Sie die Verbindung örtlich mittels des Telnet Hyperterminals.*
- L2TP oder IPSec werden nicht aufgebaut.
  - *Überprüfen Sie die Ursache im System Log.*
- Wie erkenne ich, dass EDGE funktioniert?
  - *Erfolgt das Herunterladen schneller als 85,6 kb/s, dann funktioniert EDGE.*

11. Kundenbetreuung

Aktuelle Informationen über das Produkt finden Sie auf der Seite: www.conel.cz



Wartung – Tipps:
Mit der SIM Karte sollte man genauso vorsichtig umgehen, wie mit einer Kreditkarte. Biegen Sie die Karte nicht, schützen Sie die Karte vor Beschädigung und setzen Sie die Karte nicht statischer Elektrizität aus.
Bei der Reinigung des Gerätes verwenden Sie keine aggressiven Chemikalien oder scheuernde Reinigungsmittel!

Zulassung
Die Gesellschaft Conel s.r.o. erklärt hiermit, dass das in diesem Handbuch beschriebene Gerät alle Grundanforderungen der Richtlinie 1999/5/EG (R&TTE) für den Betrieb in den Ländern der Europäischen Gemeinschaft erfüllt.





Die Konformitätserklärungen wurden ausgegeben und können beim Hersteller eingesehen werden.

12. Hinweise zur Handhabung von elektrischem Abfall

Dieses Produkt darf nicht in den Haushaltsmüll entsorgt werden. Es ist die Verpflichtung des Benutzers, den so gekennzeichneten Abfall an einer dafür bestimmten Recycling Sammelstelle für elektrische und elektronische Anlagen abzugeben. Das Sortieren und Recyceln von solchem Abfall hilft mit, die Umwelt sauber zu erhalten und stellt eine solche Art des Recyclings sicher, der die menschliche Gesundheit und Umwelt schützt. Weitere Informationen über die Möglichkeiten der Abfallentsorgung zum Recycling erhalten Sie am zuständigen Gemeinde- oder Stadtamt, bei einer sich mit der Abfallwirtschaft beschäftigenden Firma, auf den Webseiten der Sammelsysteme, auf dem Internetportal des Umweltministeriums oder bei der Firma, wo Sie das Produkt gekauft haben.



13. Vorgehensweise bei Reklamationen

Sehr geehrter Kunde,

das von Ihnen gekaufte Produkt wurde beim Hersteller etwaigen Tests unterzogen und vor dem Verkauf wurden alle Funktionen erneut von unserem Techniker überprüft. Sollte bei diesem Produkt trotz aller oben angeführten Maßnahmen eine Störung während der Garantiefrist auftreten, wegen der das Produkt nicht ordnungsgemäß weiter genutzt werden kann, bitten wir Sie, bei der Geltendmachung der Beanstandung diese Vorgehensweise bei Reklamationen zu beachten.

Zur Erleichterung eines eventuellen Beanstandungsverfahrens vergewissern Sie sich bei der Produktübernahme, ob der Händler, bei dem Sie das Produkt kaufen, die entsprechenden Stellen des Garantiescheins samt Verkaufsdatum, Stempel und Unterschrift ordentlich ausgefüllt hat.

Diese Vorgehensweise bei Reklamationen bezieht sich auf die eingekauften Produkte. Diese Vorgehensweise bei Reklamationen bezieht sich nicht auf die geleisteten Dienste.

Garantiefristen für die Produkte

Auf das eingekaufte Gerät, Versorgungsnetzteil, Datenkabel und etwaiges Zubehör wird eine Garantie von 24 Monaten ab Verkaufsdatum gewährt. Der Verkaufstag ist gleichzeitig der Tag der Produktübernahme seitens des Kunden.

Geltendmachung der Reklamation

Die Reklamation ist beim Händler, bei dem der Gegenstand der Reklamation eingekauft wurde, geltend zu machen. Bei der Reklamation legt der Kunde den ordentlich ausgefüllten Garantieschein sowie den kompletten Reklamationsgegenstand vor. Der Reklamationsgegenstand sollte in dem Zustand, der dem Zustand beim Verkauf entspricht, vorgelegt werden.

Hinweis!
Der Händler übernimmt keine Haftung für individuelle Einstellungen oder für die im Reklamationsgegenstand gespeicherten Angaben.

Bei der Geltendmachung der Reklamation ist der Kunde verpflichtet, genau anzuführen, um welche Mängel des Reklamationsgegenstandes es sich handelt bzw. auf welche Weise sich die Mängel auswirken sowie welches Recht der Haftung für Mängel er geltend macht.

Erledigung der Reklamation

Je nach Umständen stellt der Händler eine kostenlose Mängelbeseitigung sicher bzw. tauscht den Reklamationsgegenstand gegen ein neues Produkt aus bzw. erledigt die Beanstandung auf eine andere Weise in Übereinstimmung mit dem Bürgerlichen Gesetzbuch und mit dem Verbraucherschutzgesetzt.

Im Moment der Geltendmachung der Reklamation seitens des Kunden und durch die Übernahme des Beanstandungsgegenstands seitens des Händlers wird die Garantiefrist unterbrochen. Die Garantiefrist setzt sich ab dem Tag fort, an dem der Kunde den reparierten Reklamationsgegenstand oder das ausgetauschte einwandfreie Produkt übernommen hat oder bei nicht erfolgter Übernahme seitens des Kunden ab dem Tag, an dem der Kunde

verpflichtet gewesen wäre, den reparierten Reklamationsgegenstand oder das ausgetauschte Produkt zu übernehmen. Sollte der Händler im Falle der Geltendmachung eines Garantiemangels den fehlerhaften Reklamationsgegenstand gegen ein neues Produkt (samt dem Austausch der IMEI) austauschen, geht der ursprüngliche Reklamationsgegenstand somit in das Eigentum des Händlers und das neue Produkt in das Eigentum des Käufers über. Ab der Übernahme des neuen Produkts fängt die neue Garantiefrist an zu laufen. Falls der Händler laut Vereinbarung mit dem Kunden die Reklamation mit dem Austausch des Reklamationsgegenstandes gegen ein einwandfreies Produkt erledigt, geht die neue Garantie auf das Produkt zu Ende, wie folgt:

1. Nach dem Ablauf von 12 Monaten ab dem Tag der Übernahme des neuen Produkts durch den Kunden.
2. An dem Tag, an dem die Garantiefrist für das ursprüngliche Produkt (Reklamationsgegenstand) hätte ablaufen sollen, wenn der Austausch des Produkts nicht erfolgt wäre, und zwar am nachfolgenden Tag.
3. Um eine unberechtigte Reklamation handelt es sich dann, falls der beanstandete Produktmangel vom Händler im Rahmen der Reklamation nicht festgestellt wird oder sobald es sich um einen Produktmangel handelt, auf den sich nicht die Garantie im Sinne von Artikel 4 dieser Vorgehensweise bei Reklamationen bezieht
4. Wird der beanstandete Mangel nicht festgestellt und wird die Funktionstüchtigkeit des Reklamationsgegenstandes dem Kunden vorgeführt, ist der Kunde verpflichtet, die nachweisbaren, im Zusammenhang mit der sachkundigen Begutachtung des beanstandeten Mangels entstandenen Kosten zu erstatten.
5. Falls bei der Überprüfung der Berechtigung der Reklamation ein Produktmangel festgestellt wird, auf den sich nicht die Garantie (Reparatur außerhalb der Garantie) bezieht, informiert der Händler den Kunden über diese Tatsache und der Kunde teilt dem Verkäufer/Händler mit, ob er sich die Beseitigung dieses Mangels für den vom Händler verlangten Preis wünscht. Bezüglich der genauen Reparaturbedingungen außerhalb der Garantiefrist wird eine Niederschrift verfasst, die sowohl vom Kunden als auch vom Händler mit ihren Unterschriften bestätigt wird. Verlangt der Kunde die Reparatur der Mängel außerhalb der Garantiefrist zu den Bedingungen, die ihm der Händler mitteilt, wird das Gerät dann an den Kunden zurückgegeben, wenn der Kunde die nachweisbaren, im Zusammenhang mit der sachkundigen Begutachtung des beanstandeten Mangels entstandenen Kosten erstattet.

Die Garantie bezieht sich nicht auf Mängel, die entstanden sind

1. durch mechanische Beschädigung (z. B. durch einen Sturz usw.).
2. durch die Anwendung von ungeeigneten bzw. für dieses Produkt nicht empfohlenen Versorgungsnetzteilen sowie vom anderen Zubehör in Verbindung mit der Nutzung des Produkts mit nicht standardmäßigem Zubehör.
3. durch Installation oder durch Benutzung des Produkts im Widerspruch mit der Bedienungsanleitung oder durch die Benutzung des Produkts für andere Zwecke, als bei diesem Typ üblich ist.
4. durch unsachgemäße Handhabung bzw. durch den Eingriff in das Produkt durch eine unbefugten Person oder ein anderes als vom Hersteller zugelassenes Service Center.
5. durch Beschädigung infolge von höherer Macht (Hochwasser, Brandfall usw.) oder infolge von anderen örtlichen Erscheinungen (Sturm, Netzüberspannung usw.).
6. durch Lagerung außerhalb des Temperaturbereiches.

7. durch Benutzung in chemisch aggressiver Umgebung.

Sonstige Reklamationsbedingungen

Für einen Mangel wird nicht die Tatsache gehalten, dass der Reklamationsgegenstand nicht den Parametern entspricht, die für andere analoge Produkttypen gelten. Zur Beurteilung, ob es sich um einen Mangel handelt, sind die in der technischen Dokumentation zum Produkt angeführten Produktparameter maßgebend.

Die Garantie erlischt in dem Falle, dass der Reklamationsgegenstand geändert wird oder wenn die Herstellungsnummer des Reklamationsgegenstandes beschädigt oder auf andere Weise unlesbar ist.

14. Garantieschein

Gerätetyp	
Herstellungsnummer	
Garantiefrist (in Monaten)	
Händler	
Verkaufsdatum	
Stempel des Händlers	

	11	2	3	4	5
Datum der Reklamationsannahme durch den Händler					
Nummer des Reklamationsprotokolls					
Datum der Geräteannahme im Service Center					
Datum der Beendigung der Reparatur im Service Center					
Nummer des Reparaturscheins des Service Centers					
Garantiereparatur	**JA – NEIN**	**JA – NEIN**	**JA – NEIN**	**JA – NEIN**	**JA – NEIN**
Neue Herstellungsnummer des Gerätes (IMEI)					
Anmerkungen					
Stempel des Service Centers					

LUCOM GmbH * Ansbacher Str. 2a * 90513 Zirndorf * Tel. 09127/59 460-10 * Fax. 09127/59 460-20 * www.lucom.de